教育部高等学校网络空间安全专业教学指导委员会
中 国 计 算 机 学 会 教 育 专 业 委 员 会
共同指导

网络空间安全重点规划丛书

顾问委员会主任：沈昌祥　编委会主任：封化民

隐密的原理及应用

杨世勇　编著

Cyberspace Security

根据教育部高等学校信息安全专业教学指导委员会编制的
《高等学校信息安全专业指导性专业规范》组织编写

清华大学出版社

网络空间安全重点规划丛书

隐密的原理及应用

杨世勇　编著

清 华 大 学 出 版 社
北　京

内 容 简 介

本书分为 3 篇：基础篇(第 1～4 章)以隐密的原理为中心，主要介绍信息隐藏相关背景知识及数学模型；水印篇(第 5～9 章)围绕数字认证和数字追踪，主要介绍作者在数字版权保护方面的研究成果以及该技术未来的发展趋势；隐密通信篇(第 10～12 章)主要介绍在网络环境下，如何利用信息隐密技术解决通信内容的信息泄露问题。另外，本书对近些年发展很快的 PC 系统以及移动手机 App 应用系统的个人隐私保护提出了新的隐密解决方案，并全面展示了新的研究成果。

全书内容丰富翔实，涉及信息论、密码学、数字图像处理、音/视频压缩编码技术、人工智能算法等，覆盖的知识领域广，理论与实践应用密切结合，可作为信息安全、网络空间安全等相关专业的本科生、硕士或博士研究生的教材，也是值得推荐给相关领域的科研和技术人员的参考读物。

图书在版编目(CIP)数据

隐密的原理及应用/杨世勇编著. —北京：清华大学出版社，2020.1
(网络空间安全重点规划丛书)
ISBN 978-7-302-54302-2

Ⅰ. ①隐…　Ⅱ. ①杨…　Ⅲ. ①信息安全－安全技术　Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2019)第 271770 号

责任编辑：张　民　常建丽
封面设计：常雪影
责任校对：焦丽丽
责任印制：杨　艳

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-83470236
印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：13.25　　**字　　数**：317 千字
版　　次：2020 年 5 月第 1 版　　**印　　次**：2020 年 5 月第1 次印刷
定　　价：45.00 元

产品编号：083895-01

网络空间安全重点规划丛书

编审委员会

出版说明

21 世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继 2001 年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量具有前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。系列教材的作者都是既在本专业领域有深厚的学术造诣，又在教学第一线有丰富的教学经验的学者、专家。

该系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

在全力做好本版教材，满足学生用书的基础上，还经由专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入系列教材中，以进一步满足大家对外版书的需求。“高等院校信息安全专业系列教材”已于 2006 年年初正式列入普通高等教育“十一五”国家级教材规划。

2007 年 6 月，教育部高等学校信息安全类专业教学指导委员会成立大会

暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展起到重要的指导和推动作用。2006 年教育部给武汉大学下达了"信息安全专业指导性专业规范研制"的教学科研项目。2007 年起该项目由教育部高等学校信息安全类专业教学指导委员会组织实施。在高教司和教指委的指导下，项目组团结一致，努力工作，克服困难，历时 5 年，制定出我国第一个信息安全专业指导性专业规范，于 2012 年年底通过经教育部高等教育司理工科教育处授权组织的专家组评审，并且已经得到武汉大学等许多高校的实际使用。2013 年，新一届教育部高等学校信息安全专业教学指导委员会成立。经组织审查和研究决定，2014 年以教育部高等学校信息安全专业教学指导委员会的名义正式发布《高等学校信息安全专业指导性专业规范》(由清华大学出版社正式出版)。

2015 年 6 月，国务院学位委员会、教育部出台增设"网络空间安全"为一级学科的决定，将高校培养网络空间安全人才提到新的高度。2016 年 6 月，中央网络安全和信息化领导小组办公室(下文简称中央网信办)、国家发展和改革委员会、教育部、科学技术部、工业和信息化部及人力资源和社会保障部六大部门联合发布《关于加强网络安全学科建设和人才培养的意见》(中网办发文〔2016〕4 号)。2019 年 6 月，教育部高等学校网络空间安全专业教学指导委员会召开成立大会。为贯彻落实《关于加强网络安全学科建设和人才培养的意见》，进一步深化高等教育教学改革，促进网络安全学科专业建设和人才培养，促进网络空间安全相关核心课程和教材建设，在教育部高等学校网络空间安全专业教学指导委员会和中央网信办资助的网络空间安全教材建设课题组的指导下，启动了"网络空间安全重点规划丛书"的工作，由教育部高等学校网络空间安全专业教学指导委员会秘书长封化民教授担任编委会主任。本规划丛书基于"高等院校信息安全专业系列教材"坚实的工作基础和成果、阵容强大的编审委员会和优秀的作者队伍，目前已经有多本图书获得教育部和中央网信办等机构评选的"普通高等教育本科国家级规划教材""普通高等教育精品教材""中国大学出版社图书奖"和"国家网络安全优秀教材奖"等多个奖项。

"网络空间安全重点规划丛书"将根据《高等学校信息安全专业指导性专业规范》(及后续版本)和相关教材建设课题组的研究成果不断更新和扩展，进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着我国网络空间安全学科的发展不断完善，力争为我国网络空间安全相关学科专业的本科和研究生教材建设、学术出版与人才培养做出更大的贡献。

我们的 E-mail 地址是：zhangm@tup.tsinghua.edu.cn，联系人：张民。

"网络空间安全重点规划丛书"编审委员会

前　言

在互联网应用时代，大数据和云计算为海量数据分布式存储、智能搜索提供了便利，但同样也为用户的隐私带来潜在的安全威胁。诸如用户的重要数据、私密以及敏感信息等容易被搜集、转存，而且一旦泄露并被散布是很难可逆追踪的。因此，个人计算机、手机以及各种电子终端设备中用户隐私的保护也成了大众不得不考虑的问题。

基于互联网的各种即时通信软件存在被搭线窃听的问题，致使通信的内容被第三方非法侦听。犯罪分子利用盗取的信息进行模仿、诱导、实施网络诈骗，使公众蒙受巨大的财产损失。有人甚至惊呼，在数字网络时代，人们似乎都住在了“玻璃房子”而无处遁形！信息保密问题无疑成了公众关注的热点之一。

密码学(Cryptography)是传统的保密方法之一。但近些年，隐写术(Stegnography)或者信息隐藏(Information Hiding)技术的兴起，为保密技术带来了另一种全新的思路。

本书之所以命名为“隐密”，主要是为了与“加密”对应。也就是说，将信息隐藏和密码学作为一个层次上的概念，将隐密和加密作为另一个层次上的概念比照。广义上，无论是密码学中的加密(Encryption)，还是信息隐藏中的隐密(Hiding)，都属于保密技术的范畴。

作为一种有特点的保密技术，我们简单地用5A概括隐密的特征。时效性(Any-time)：时间上不能确认什么时候发生。随机性(Any-where)：空间上不能确认发生在哪里。欺骗性(Any-how)：手法上不能确认以什么方式发生。模糊性(Any-what)：感官上不可捉摸。和谁发生通信(Anyone)：对象上的隐匿性。类似地，可以把这些A扩展到无穷维度上。

如今的隐密技术已经逐渐被越来越多的应用领域所关注。

- 政府OA系统：政府办公重要文件内容的安全保护，敏感文件的保密传输。
- 情报部门：涉外机构搜索的敏感情报可采取隐密的方式进行秘密传达。
- 公安领域：公安部门的行动指令等可采取隐密的传输手段，避免被犯罪分子反侦听。
- 军事领域：军事通信部门需要将行动命令以及(真伪)识别信息隐藏

于正常的通信调度内容中。

- 金融领域：金融系统的数据需要采取隐密传输方式保证其在通信过程中安全。
- 媒体传播领域：广电媒体可利用电视节目作为载体，使用隐密传输技术传输敏感或重要的数据内容。
- 电子商务领域：电子商务系统也有必要采取有效的隐密技术保护用户个人的数据隐私。
- 企事业单位文件管理系统：大型企业内部隐私数据（竞标书等）的传输也同样需要掩蔽保护。

相信未来隐密技术的发展还会有更广阔的应用空间。很显然，随着网络通信技术及相关技术的不断发展，信息保密安全面临各方的潜在挑战，我们仍需要不断研究、挖掘新的隐密应用技术满足公众对安全保密的诉求。

本书主要有3个方面的特点。其一，延续性：作者一直致力于信息隐藏领域的研究工作，书中的内容既是对个人20年研究成果的总结，也是信息隐藏这门学科这么多年发展历程的一个侧面体现。其二，本书注重理论和实际相结合：基于信息论和统计学的观点，对国际、国内该领域已有的研究成果加以分析、对比以及总结。在理论的指导下，结合实际，给出实践中大量的应用范例。其三，侧面体现了信息隐藏学科最近的发展成果：以前该领域大多数研究结果都围绕数字认证，本书还将网络即时隐密通信，以及手机移动终端的个人隐私保护作为研究内容加以重点推广，具有技术上的超前性。

编写本书的目的是向读者介绍隐密的基本理论和应用方法。这门技术融合了密码学、信息论、网络通信、多媒体处理、人工智能、心理学、感官艺术甚至哲学等方面的发展成果，不得不说是一门交叉性比较强的学科。因此，对于读者，要深刻理解本书中的内容，也许需要别的一些书籍或者专业知识做铺垫。

本书可作为信息安全、网络空间安全等相关专业的本科生、硕士或博士研究生的教材。

在本书的编写过程中，博士生兰慧仔细校对并整理了全书的初稿，提出了不少宝贵的修改意见，她对书稿付出了辛勤劳动并做出很大贡献，在此向她表示衷心的感谢！

本书得到国家自然科学基金项目（基于分层超完备字典系数表示的深度学习算法研究及应用，项目号：90308140034）、陕西省重大科技攻关项目（涉密信息输入输出安全防护管理系统）的资助，特此致谢。

编　者
2019年10月

目 录

基 础 篇

水　印　篇

隐密通信篇

基 础 篇

基础篇以隐密的原理为中心，主要介绍信息隐藏相关背景知识及数学模型。这部分内容主要在第1～4章中讲述。其中，第1章以信息论为基础，探讨隐密的理论知识；第2章以编码、密码学加密为主，介绍相关的保密研究模型；第3章论述在水印认证码中隐密的相关数学知识；第4章提出并证明完善的信息隐藏方案及算法。

第 1 章 背景知识

1.1 概率与随机分布

定义：假设 X 和 Y 是随机变量，用 $p(x)$ 表示 X 取值为 x 的概率，用 $p(y)$ 表示 Y 取值为 y 的概率。

联合概率：$p(x,y)$ 是 X 取值为 x 且 Y 取值为 y 的概率。

条件概率：$p(x \mid y)$ 表示给定 Y 取值为 y 时 X 取值 x 的概率。

联合概率和条件概率的关系：$p(x,y) = p(x \mid y)p(y)$。

这里，x 和 y 可互换，即 $p(x,y) = p(y \mid x)p(x)$。

如果对于任意 $x \in X, y \in Y, p(x,y) = p(x)p(y)$ 都成立，则称 X 和 Y 是相互独立的。

定理 1.1(贝叶斯定理)：如果 $p(x) > 0, p(y) > 0$，那么

$$p(x \mid y) = \frac{p(x)p(y \mid x)}{p(y)} = \frac{p(y)p(x \mid y)}{p(x)} \tag{1-1}$$

推论 1.1：如果 X 和 Y 是独立变量，当且仅当对所有的 x 和 y，都有 $p(x \mid y) = p(x)$ 或者 $p(y \mid x) = p(y)$，即如果两个随机变量独立，那么在观察任意一个随机变量条件下，另外一个变量的概率不会因此改变。

定义：统计偏差。

令 P 和 Q 为两个在支撑域 Ω 上的离散概率分布，$a \in \Omega$，则

$$d(P,Q) = \sum_{a \in \Omega} \mid P(a) - Q(a) \mid \tag{1-2}$$

为概率分布 P 和 Q 的统计偏差。

定义：不可区分性。如果随机序列 $\{P_n\}$ 和 $\{Q_n\}$ 在取值域 Ω 上是统计上不可区分的，则函数 $d(P_n,Q_n) \to \varepsilon_n$，其中 ε_n 为任意小的正数。也可称序列 $\{P_n\}$ 和 $\{Q_n\}$ 是统计上可忽略的。

1.2 熵、联合熵、条件熵、相对熵以及互信息

定义：令 X 是具有字符集 $\boldsymbol{X}$ 的离散随机变量，其概率密度函数

$$P(x) = P_r\{X = x\}, \quad x \in X$$

则 X 的熵 $H(X)$ 为

$$H(X)=-\sum_{x\in X}p(x)\log_2 p(x) \tag{1-3}$$

定义：用 E 表示期望值。如果 $X\sim P(x)$，则随机变量 $g(X)$ 的期望值可记为

$$E_P g(X)=\sum_{x\in X}g(x)p(x)。 \tag{1-4}$$

特别地，当 $g(x)=\log_2\dfrac{1}{p(x)}$ 时，则

$$H(X)=E_P\log_2\frac{1}{p(X)} \tag{1-5}$$

因为 $0\leqslant p(x)\leqslant 1$ 意味着 $\log_2(1/p(x))\geqslant 0$，因此 $H(X)\geqslant 0$。

(1) **联合熵**(Joint Entropy)

一对具有联合分布 $p(X,Y)$ 的离散随机变量 X,Y 的联合熵定义为

$$H(X,Y)=-\sum_{x\in X}\sum_{y\in Y}p(x,y)\log_2 p(x,y) \tag{1-6}$$

也可表示为

$$H(X,Y)=-E_{P(x,y)}\log_2 p(X,Y) \tag{1-7}$$

(2) **条件熵**(Conditional Entropy)

如果 $X,Y\sim p(x,y)$，则条件熵 $H(Y\mid X)$ 可定义为

$$\begin{aligned}H(Y\mid X)&=\sum_{x\in X}p(x)H(Y\mid X=x)\\&=\sum_{x\in X}p(x)\sum_{y\in Y}p(x\mid y)\log_2 p(y\mid x)\\&=\sum_{x\in X}\sum_{y\in Y}p(x,y)\log_2 p(y\mid x)\\&=-E_{p(x,y)}\log_2 p(Y\mid X)\end{aligned} \tag{1-8}$$

(3) **联合熵和条件熵的关系**

$$H(X,Y)=H(X)+H(Y\mid X) \tag{1-9}$$

等效地，

$$\log_2 p(X,Y)=\log_2 p(X)+\log_2 p(Y\mid X) \tag{1-10}$$

推论：

$$H(X,Y\mid Z)=H(X\mid Z)+H(Y\mid X,Z) \tag{1-11}$$

(4) **相对熵**(Relative Entropy)

两个概率密度函数 $p(x)$ 和 $q(x)$ 之间的相对熵定义为

$$\begin{aligned}D(p\,||\,q)&=\sum p(x)\log_2\frac{p(x)}{q(x)}\\&=E_p\log_2\frac{p(X)}{q(X)}\end{aligned} \tag{1-12}$$

(5) **互信息**(Mutual Information)

如果 $X\sim p(x)$，$Y\sim p(y)$ 且 X 和 Y 具有联合概率分布 $X,Y\sim p(x,y)$，则定义 X 和 Y 的互信息 $I(X;Y)$ 为

$$I(X;Y)=\sum_{x\in X}\sum_{y\in Y}p(x,y)\log_2\frac{p(x,y)}{p(x)p(y)}$$

$$= D(p(x,y)\ ||\ p(x)p(y))$$

$$= E_{p(x,y)}\log_2 \frac{p(X,Y)}{p(X)p(Y)} \tag{1-13}$$

推论：联合熵和互信息之间的关系为

$$I(X;Y) = H(X) - H(X \mid Y) \tag{1-14}$$

也就是说，互信息 $I(X;Y)$ 是 X 的不定性因为 Y 的背景知识而下降。

1.3 熵、条件熵、相对熵以及互信息的链规则

定理：(熵链)令随机变量 $X_1, X_2, \cdots, X_n$ 符合概率 $p(x_1, x_2, \cdots, x_n)$ 分布，于是

$$H(X_1, X_2, \cdots, X_n) = \sum_{i=1}^{n} H(X_i \mid X_{i-1}, \cdots, X_n) \tag{1-15}$$

定义：(条件熵链)在给定 Z 的条件下，随机变量 X 和 Y 的条件熵可定义为

$$I(X;Y \mid Z) = H(X \mid Z) - H(X \mid Y, Z)$$

$$= E_{p(x,y,z)}\log_2 \frac{p(X,Y \mid Z)}{p(X \mid Z)p(Y \mid Z)} \tag{1-16}$$

定理：(信息链)

$$I(X_1, X_2, \cdots, X_n; Y) = \sum_{i=1}^{n} I(X_i; Y \mid X_{i-1}, X_{i-2}, \cdots, X_1) \tag{1-17}$$

定义：条件相对熵 $D(p(y \mid x)\ ||\ q(y \mid x))$ 是条件概率密度函数 $p(y \mid x)$ 和 $q(y \mid x)$ 在概率密度函数 $p(x)$ 上的相对熵的平均。

$$D(p(y \mid x)\ ||\ q(y \mid x)) = \sum_x p(x) \sum_y p(y \mid x) \log \frac{p(y \mid x)}{q(y \mid x)} \tag{1-18}$$

定理：(相对熵的链规则)

$$D(p(x,y)\ ||\ q(x,y)) = D(p(x)\ ||\ q(x)) + D(p(y \mid x)\ ||\ q(y \mid x)) \tag{1-19}$$

1.4 熵的某些特性

定理：令 $p(x), q(x), x \in X$，为两个概率密度函数，于是

$$D(p\ ||\ q) \geqslant 0 \tag{1-20}$$

当且仅当对所有 $x, p(x) = q(x)$ 都成立。

推论：(互信息的非负性)对于任意两个随机变量 X、Y，都有

$$I(X;Y) \geqslant 0 \tag{1-21}$$

当且仅当 X 和 Y 相互独立时，该式中等号的情况成立。

推论：$D(p(y \mid x)\ ||\ q(y \mid x)) \geqslant 0$。

当且仅当，对于所有具有 $p(x) > 0$ 的 y 和 x 都有 $p(y \mid x) = q(y \mid x)$。

推论：$I(X;Y \mid Z) \geqslant 0$，当且仅当，在给定 Z 的条件下，y 和 x 相互独立时等号成立。

定理：$H(X) \leqslant \log_2 \mid X \mid$。这里，$X$ 为定义范围 $\mid X \mid$ 中的数，当且仅当 X 在定义域

X 上均匀分布时等号成立。

定理：(条件降低熵) $H(X \mid Y) \leqslant H(X)$，当且仅当 X 和 Y 相互独立时等号成立。

定理：(熵的独立界)令随机变量 $X_1, X_2, \cdots, X_n$ 符合概率 $p(x_1, x_2, \cdots, x_n)$ 分布，于是，

$$H(X_1, X_2, \cdots, X_n) \leqslant \sum_{i=1}^{n} H(X_i) \tag{1-22}$$

当且仅当所有 X_i 相互独立时等号成立。

随机过程 $\{X_i\}$ 的熵率被定义为

$$H(X) = \lim_{n \to \infty} \frac{1}{n} H(X_1, X_2, \cdots, X_n) \tag{1-23}$$

当等号右面的熵极限存在时。

1.5 马尔可夫链

定义：离散随机过程 $X_1, X_2, \cdots$ 被称为马尔可夫(Markov)链或者马尔可夫过程，对于 $i = 1, 2, \cdots, n$ 以及 $x_1, x_2, \cdots, x_n, x_{n+1} \in X$，都有

$$\begin{aligned} &P_r(X_{n+1} = x_{n+1} \mid X_n = x_n, \mid X_{n-1} = x_{n-1}, \cdots, X_1 = x_1) \\ &= P_r(X_{n+1} = x_{n+1} \mid X_n = x_n) \end{aligned} \tag{1-24}$$

在这种情况下，随机变量的联合概率密度函数可写为

$$p(x_1, x_2, \cdots, x_n) = p(x_1) p(x_2 \mid x_1) p(x_3 \mid x_2) \cdots p(x_n \mid x_{n-1}) \tag{1-25}$$

定义：Markov 链被称为是非时变的，如果条件概率 $p(x_{n+1} \mid x_n)$ 不依赖于 n，也就是对于 $n = 1, 2, \cdots$ 以及所有 $a, b \in X$，都有

$$P_r(X_{n+1} = b \mid X_n = a\} = P_r\{X_2 = b \mid X_1 = a)\} \tag{1-26}$$

(1) 如果 $\{X_i\}$ 是一 Markov 链，则 X_n 被称为在时间 n 时的状态。一个非时变的 Markov 链可以用它的初始状态和概率转移矩阵 $P = \lfloor P_{ij} \rfloor, i, j \in \{1, 2, \cdots, m\}$ 描述。这里，m 表示可能的状态数，$P_{ij} = P_r\{X_{n+1} = j \mid X_n = i\}$。

(2) 如果随机变量的概率密度函数在时间 n 的概率为 $p(x_n)$，则概率密度函数在时间 $n+1$ 可表示为

$$p(x_{n+1}) = \sum_{x_n} p(x_n) P_{x_n x_{n+1}} \tag{1-27}$$

(3) 如果 $X \to Y \to Z$ 形成一 Markov 链，则

$$I(X;Y) \geqslant I(X;Z) \text{ 以及 } I(X;Y \mid Z) \leqslant I(X;Y) \tag{1-28}$$

1.6 Jensen 不等式

如果 f 是一凹函数，X 是一随机变量，则

$$E(f(X)) \geqslant f(E(X)) \tag{1-29}$$

进一步，如果 f 是严格凹的，上面不等式中等号成立意味着 X 是一常量。

1.7 Fano 不等式

假设要估计一个具有 $p(x)$ 分布的随机变量 X。观察一个通过条件概率 $p(y \mid x)$ 和 X 联合分布的随机变量 Y，记 $\hat{X}=g(Y)$ 为通过 Y 对 X 的估计。若想约束错误 $\hat{X} \neq X$ 的概率，定义错误概率 $P_e = P_r\{X \hat{\neq} X\}$，则

$$H(P_e)+P_e\log_2(|X|-1) \geqslant H(X \mid Y) \tag{1-30}$$

Fano 不等式可以弱化为

$$1+P_e\log_2|X| \geqslant H(X \mid Y) \tag{1-31}$$

或者

$$P_e \geqslant \frac{H(X \mid Y)-1}{\log_2|X|} \tag{1-32}$$

注意：$P_e=0$ 意味着 $H(X \mid Y)=0$，即直觉猜想没有任何错误。

1.8 Chernoff 界

令 $X_1, X_2, \cdots, X_n$ 为 n 个独立同分布的伯努利(Bernoulli)变量，具有相同的期望值 p。于是，对于任意 $0<\varepsilon<1$，

$$P_r\left[\frac{1}{n}\sum_{i=1}^{n}X_i \geqslant \varepsilon\right] \leqslant \mathrm{e}^{-nD(\varepsilon,p)} \quad \varepsilon \geqslant p \tag{1-33}$$

$$P_r\left[\frac{1}{n}\sum_{i=1}^{n}X_i \leqslant \varepsilon\right] \leqslant \mathrm{e}^{-nD(\varepsilon,p)} \quad \varepsilon \leqslant p \tag{1-34}$$

这里，$D(x,y)=x\log_2\left(\frac{x}{y}\right)+(1-x)\log_2\left(\frac{1-x}{1-y}\right)$ 是一个凹的在 $0<x,y<1$ 域上非负的函数，仅当 x 和 y 相等时等号成立。

注意：以后如不特别声明，所有的 log 函数都以 2 为底。

第 2 章 加密及隐密的通信模型

2.1 一般的通信系统

一般的通信系统框图如图 2-1 所示。

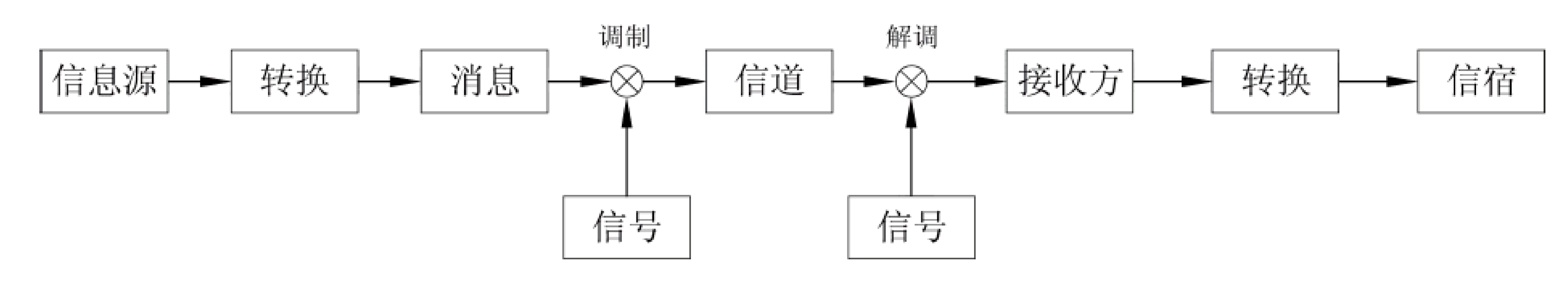


图 2-1 一般的通信系统框图

发送端：发送方或者编码器将从信息源来的信号转换成消息编码序列，而且利用当地产生的载波信号将消息调制（如果是基带信号传输，则不存在调制和解调）转换成能够传输的数字信号，然后发送到信道。

接收端：接收方或者解码器将收到的调制数字信号进行解调重新生成原数字消息数据，最后将消息数据解码还原成源信息。

信道：作为在发送端和接收端信号的传输通道，可以是无线的，也可以是有线的，信道的物理组成称为媒介，如无线的空气，有线的同轴电缆、双绞线等，在网络环境下可以理解为收发应用之间的链路。

2.2 一般通信系统的主要元素及指标

2.2.1 数据元素与信号元素

数据元素（Data Element）：数据元素是表示一块信息的最小实体。在数据通信中，人们的目标是发送数据元素。

信号元素（Signal Element）：信号单元是数字信号的最小单元。在数字通信中，信号元素承载数据单元。

区别：数据元素是人们要发送的，而信号元素是人们能发送的。数据元素被承载，信号元素是载体。

2.2.2　数据速率与信号速率

数据速率(Date Rate)：一秒发送的信号元素(位)的数量，单位是(b/s)，有时也称为比特率(Bit Rate)。

信号速率(Signal Rate)：一秒发送的信号元素的数量，单位是(baud)，有时也称为脉冲速率(Pulse Rate)、调制速率(Modulation Rate)或波特率(Baud Rate)。

数据率和信号速率之间的关系：在数据通信中，最坏的情形是需要最大数据率，最好的情形是需要最小信号速率。一般情形下，数据率和信号速率之间的关系如下：

$$S = c \times N \times \frac{1}{r}\text{baud} \tag{2-1}$$

这里的 N 是数据速率(b/s)，c 是情形因子，S 是信号元素数量，而 r 表示每个信号元素能承载的数据元素的比值。

2.2.3　信道的带宽、数据速率及容量

最小带宽：

$$B_{\min} = c \times N \times \frac{1}{r}$$

如果给出通道带宽，则可以得到信道的速率。

最大数据速率：

$$N_{\max} = \frac{1}{c} \times B \times r$$

信道容量(Shannon 容量定理)：

$$C = B\log_2\left(1 + \frac{S}{N}\right)$$

Shannon 容量定理能够确定噪声信道理论上的最高数据速率。这里，C 代表信道容量，B 代表带宽，S 代表信号功率，N 代表噪声功率。

2.3　保密系统模型

2.3.1　Simmons“狱卒”问题及保密通信系统

Alice 和 Bob 两个人深陷图圄，他们只能利用正常信件的交流进行秘密通信，Alice 和 Bob 的信件内容看起来正常，但其中隐含了“越狱”的信息，而狱卒 Oscar 具有审查他们通信内容的权利，而且拥有足够的资源进行“盘问”和质疑。

基于 Simmons 狱卒问题的一个典型的保密通信系统(Secrecy System)模型[1] 如图 2-2 所示。

可以用一个五元组 $\Gamma=(M,C,K,E,D)$ 表示一个保密系统，Γ 主要包括以下 5 个部分。

- 明文空间 M：是明文的有限集，$m = \{m_1 m_2 \cdots m_n\}$，其中 $m \in M$，n 表示长度。
- 密文空间 C：是密文的有限集，$c = \{c_1 c_2 \cdots c_n\}$，其中 $c \in C$。

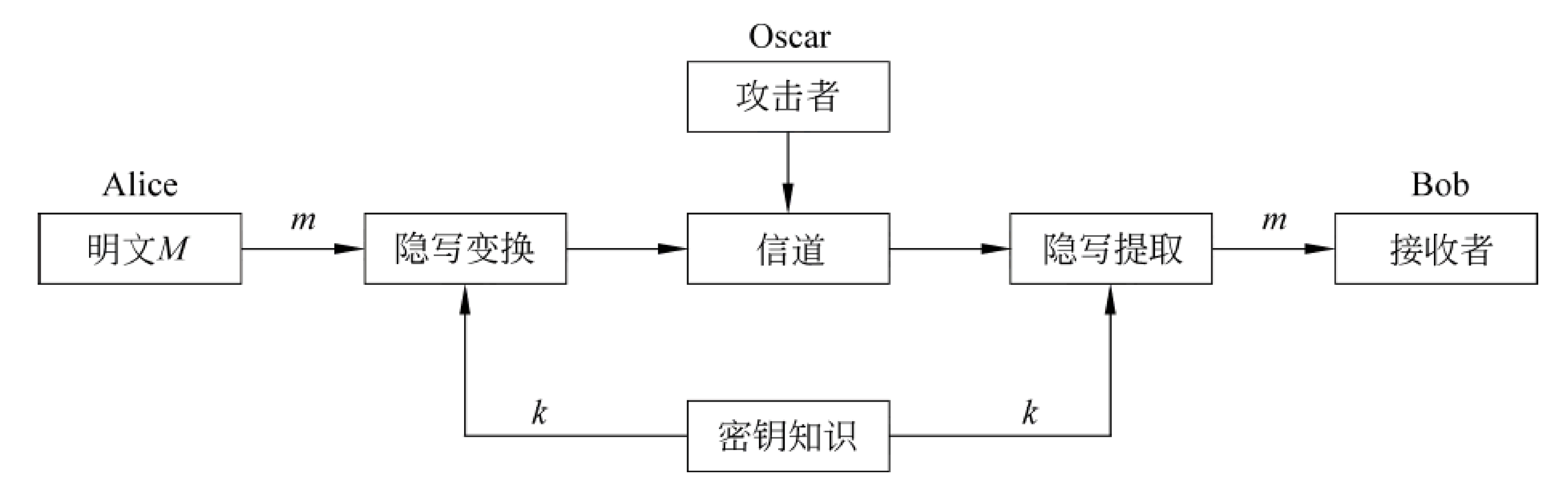


图 2-2　保密通信系统模型

- 密钥知识 K：是密钥的有限集，$k=\{k_1k_2\cdots k_n\}$，其中 $k\in K$。
- 加密函数 E：给定明文消息 $m\in M$，密钥 $k\in K$，将明文 m 变换为密文 c，即

$$c=E(m,k),\quad m\in M,\ k\in K \tag{2-2}$$

- 解密函数 D：接收者利用通过密钥信道送来密钥进行变换得到明文，即

$$m=D(c,k),\quad m\in M,\ k\in K \tag{2-3}$$

这里要注意，每个加密变换都对应一个解密变换，也就是说必须满足：

$$D_K(E_K(m))=m,\quad \forall m\in M \tag{2-4}$$

2.3.2　私钥和公钥加密体制

在 2.3.1 节提到的保密系统模型中，隐写变换和隐写提取这两个模块涉及的密钥分配方法有两种类型：一种是私钥（单钥）密码体制；一种是公钥（双钥）密码体制。

1. 私钥（单钥）密码体制

加密密钥和解密密钥相同，也就是加密使用的密钥和解密使用的是同一个密钥。按照密钥的唯一性，解密者如果要获得明文，就必须拥有正确而且唯一的加密者的私钥，如图 2-3 所示。

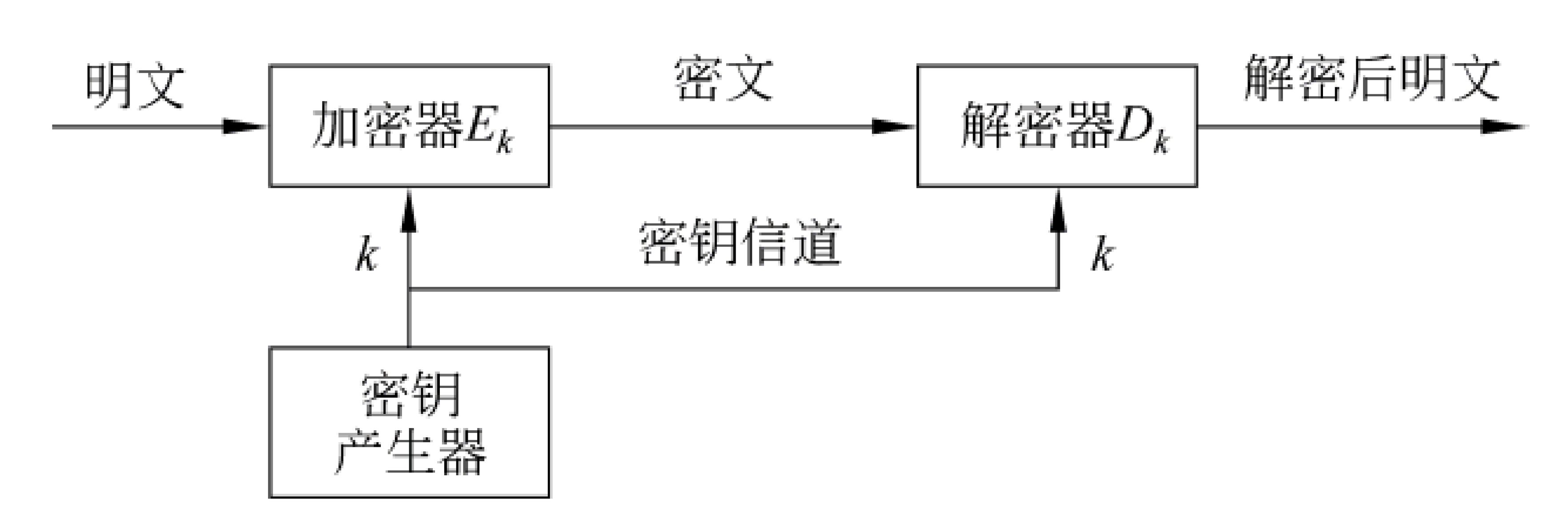


图 2-3　私钥加密系统

单钥密码体制不仅可用于数据加密，也可用于消息认证，可分为流密码和分组密码两大类。但在现代网络通信系统中，这种单钥体制有如下缺点。

- 发送者用自己的私钥加密明文获得密文发送到接收者。为了使接收者获得秘密消息，同时也需要将私钥发送给接收者，他的私钥同时被暴露。
- 为了保护隐私不被攻击，发送者只能采用一次一密的方式，这样在随机意义上是安全的，但发送者必须每加密一次，就产生新的密钥。那么，在这种加密模式下，密钥的生成、转储、保存就成了负担。
- 私钥需要另外更安全的信道进行传输。

2. 公钥密码体制

典型的公钥密码体制有 RSA 公钥加密系统，如图 2-4 所示。它由国际上著名的三位学者 R. L. Revest、A. Shamir 和 L. Adleman 发现，并已普及应用。RSA 加密的本质在于当数据位极大时，在不知陷门信息下，极难确定变(代)换之间的关系。RSA 不仅可用于加密，也可用于数字签名。

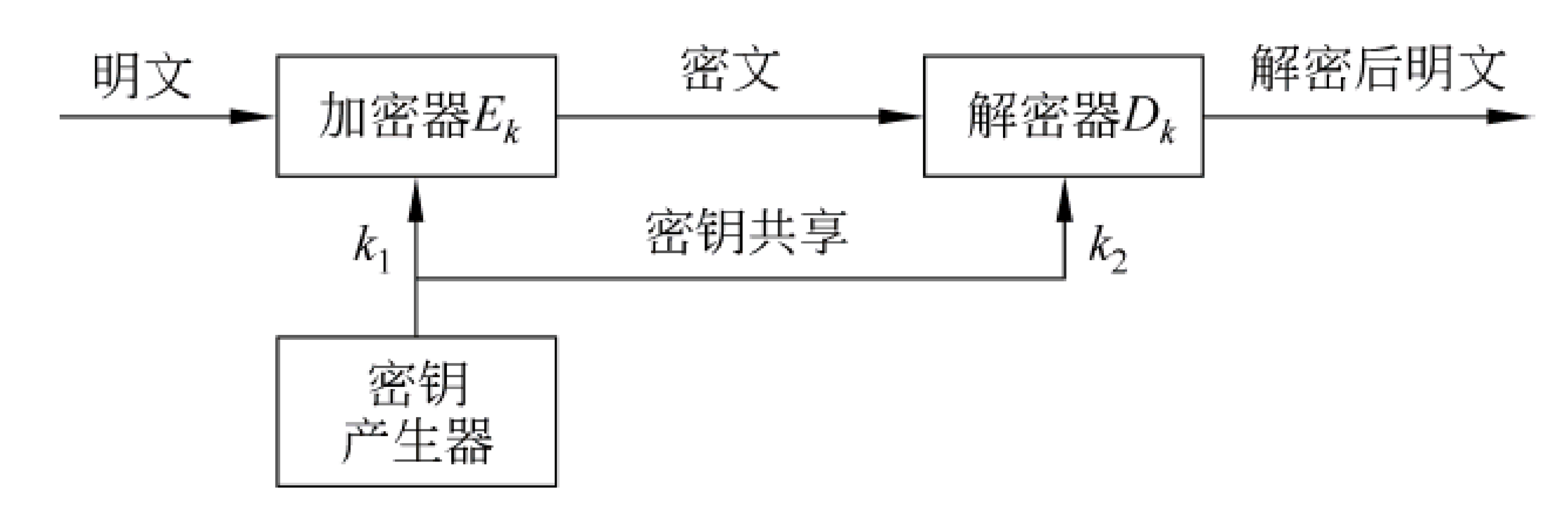


图 2-4 公钥加密系统

- 公钥体制下，加密密钥和解密密钥不同。
- 公钥体制使用的密钥对(k_1，k_2)理论上由第三者产生并提供给通信的双方。也就是说，加密使用的密钥和解密使用的密钥基于随机序列的产生和数学上的难题。可以做到加密使用的密钥和解密使用的密钥不同，但显然这一对密钥(k_1，k_2)之间有某种内在复杂的对应关系。
- 采用公钥密码模式，允许发送方和接收方在通信时临时产生会话密码。发送方不需要发送自己的私钥 k_1 到接收方，接收方用自己的私钥解密即可。这样，通信双方都防止了私钥的泄露。
- 在一对密钥中，公钥 k_2 可以是公开的用户信息，如公开电话号码等。

显然，与私钥体制相比，公钥体制采用两个密钥将加密和解密分开进行，因此它具有如下 3 个优点。

- 通信双方无须事先交换密钥，就可进行保密通信。
- 以密钥对里面包含的公钥作为加密密钥，私钥作为解密密钥，可实现多个用户加密的消息只能由一个用户解密，可用于网络保密通信。
- 将用户私钥作为加密密钥，而以公钥作为解密密钥，则可实现一个用户加密的消息由多个用户解密，可用于数字群签名。

2.3.3 加密及解密过程

假定整个明文空间 M 有一个概率分布，用 $p_M(x)$表示明文 x 发生的先验概率，密钥 k 被选择的概率表示为 $p_K(k)$，用 $p_C(y)$表示导出密文 y 的后验概率。对每个 $k\in K$，定义

$$C(k)=\{E_k(x):x\in M\} \tag{2-5}$$

即如果 k 是密钥，则 $C(k)$是可能的密文集，然后对每个 $y\in C$，加密后的密文分布概率为

$$p_C(y)=\sum_{\{k:\ y\in C(k)\}} p_K(k)\,p_M(D_K(y)) \tag{2-6}$$

另一方面，对每个 $y\in C$ 和 $x\in M$，在一定的输入下观察系统的输出，计算条件概率 $p_C(y\mid x)$（即给定 x 是明文，y 是密文的概率）为

$$p_C(y \mid x) = \sum_{\{k:\ x=D_k(K)\}} p_K(x) \tag{2-7}$$

利用贝叶斯定理，在观察系统输出下计算条件概率 $p_M(x \mid y)$（即给定密文 y 和 x 是明文的概率）为

$$p_{(}x \mid y) = \frac{p_M(x) \sum_{\{k:\ x=D_K(y)\}} p_K(k)}{\sum_{\{k:\ y\in C(k)\}} p_K(k)\, p_M(D_K(y))} \tag{2-8}$$

注意：式(2-7)和式(2-8)可用于密码分析和攻击。

2.3.4 计算保密性与完全保密性

计算保密性：当攻破一个密码体制已知最好的方法需要的计算时间过大时(限定一个超常规时限)，则称一个密码体制是"计算上保密的"。另一个提供计算保密性的方法是把一个密码体制的保密性转换为一些已经研究过的非常困难的问题。

无条件保密性：如果一个密码体制在有无限计算资源条件下都不能被破译，则将之定义为无条件保密的。

密码体制的无条件保密性显然不能根据计算复杂性研究，因为我们允许计算时间是无限的。研究无条件保密性的最合适的方法是概率论。

保密性：由 Shannon 提出，是一个 $|K|=|C|=|M|$ 的密码体制，该密码体制提供完全保密性，当且仅当每个密钥是等概 $1/|K|$ 使用的，且对每个 $x\in M$ 和 $y\in C$，都有唯一的密钥 k 满足 $D_K(x)=y$。有关此定理的证明可参考文献[2]。

定义：一个密码体制具有完全保密性，如果 $p_M(x \mid y)=p_M(x)$ 对所有 $x\in M, y\in C$ 成立，即在给定观察到的密文 y 的条件下，明文 x 的后验概率等于明文 x 的先验概率。

注意：完全保密性的一个典型实现是一次一密乱码本。

2.3.5 完善安全

定理：令 $p(M)$ 为明文消息 M 的先验概率，$p(E|M)$ 为选择明文 M 的条件概率，$p(E)$ 为获得的密文的概率，$p(E|M)$ 为 E 被截获后明文消息 M 的后验概率。对于一个完善安全的充分必要条件是：对每一 M 和 E，$p(E|M)=P(E)$ 都成立。

相反，如果 $p(E|M)=p(E)$，则可得 $p(M \mid E)=p(M)$。以上定理可通过贝叶斯定理推导为"真"。

也就是说，对于一个完善保密系统，选择明文消息 M 下的密文与明文消息 M 是相互独立的，即消息的先验概率等于后验概率。在这种条件下，保密系统对于计算是免疫的。

注意：完善的保密系统意味着能够获得完善的安全。

2.4 隐密通信系统

信息隐藏是指将一种重要信息隐藏在另一种信息中。隐密通信是信息隐藏的一种，它建立在正常通信系统的基础上。其含义是在正常通信的内容中，将重要的秘密信息(密

信)隐藏在其中,从而达到密信的潜行传送而不为人类的感官系统所觉察。

通常,一个正常的通信系统分为发送者、信道和接收者。对应地,一个隐密系统可分为隐密者(端)、信道和解密者(端)。关于这里的信道定义,一些文献把多媒体的内容作为隐密的隐藏信道(Covert Channel),而从一般通信的角度讲,也可认为是一种特殊的公共通信信道。另一些文献也把它们称为编码器、噪声信道(攻击者)以及解码器,见狱卒模型。

2.4.1 信息隐藏的通用模型

信息隐藏的通用模型如图 2-5 所示。

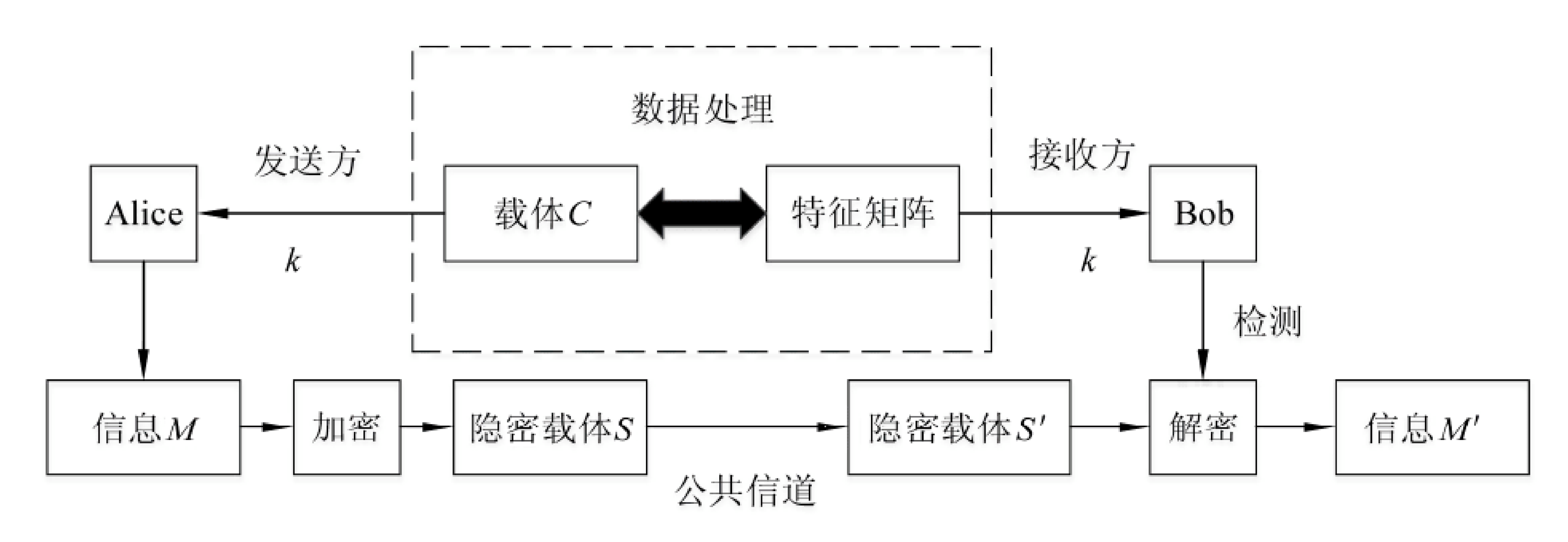


图 2-5 信息隐藏的通用模型

其中,对秘密信息的加密操作属于可选环节。若进行隐密,则对应于接收方需要进行相应的解密操作。数据处理操作是通信双方都必须执行的环节,也是能够进行隐密通信和解密的关键。

秘密信息 M (Secret Message):将要加入载体中的消息数据。秘密数据在真正隐藏到载体之前,可以通过加密变换的方式转换为类似于噪声的伪随机序列。为了增加系统的安全性,在这个阶段一般会对 M 加密,然后得到 M',进而进行后续操作。

原始载体 C (Cover):即进行隐藏的载体,如图像、音频、视频和文本等。为了达到掩饰的效果,一般情况下,秘密信息需要嵌入在载体的特征分布区域。因此,在实施真正的信息嵌入前还需要对载体的特征进行分析处理。

嵌入算法 E (Embedding Algorithm):用户通过使用密钥利用该算法将秘密信息嵌入到载体中。

载体特征 S (Stego-Text):S 是基于 C 的特征数据,$S \in C$。

提取算法 D (Extracting Algorithm):用户通过分享的密钥利用该算法将秘密信息从携载密信的载体中提取出 M。

2.4.2 攻击信道模型

攻击信道:攻击者(Oscar)可允许从无记忆信道中选择任意一个信道攻击水印,而且无论是编码器,还是解码器,事先都不能确认攻击采取的是哪个信道。隐密背景下的攻击信道如图 2-6 所示。



图 2-6　隐密背景下的攻击信道

2.4.3　隐密通信模型

基于流程图 2-5,可给出隐密通信模型的一个形式化定义,具体如下。

定义:令 $\sum(C,M,K,S,D,E)$六元组表示信息隐藏系统。C 表示原始载体,M 表示要传输的信息,K 表示隐藏系统的密钥集合,S 是指实际通信中发送的隐密载体,E 和 D 分别表示嵌入算法和提取算法,则

隐密过程:

$$E(M,K) = \sum_{m\in M,k\in K} p_{m,k}(M=m,K=k) = \sum_{s\in S} p(s) \tag{2-9}$$

解密过程:

$$D(S',K) = \sum_{s} p_{s',k}(S'=s,K=k) = \sum_{m\in M} p(m) \tag{2-10}$$

中间信道过程:

$$\sum_{s'\in S'} p(S'=s') \cong \sum_{s\in S} P(S=s) \tag{2-11}$$

注意,这里之所以把 S' 和 S 区别对待,是因为在发送者和接收者之间存在一个信道传输。信号经过信道可能会存在有限的干扰损失。在信息隐藏的背景下,也把中间的这个信道等效成攻击信道,参见狱卒模型。当然,后面还会对这个攻击信道加以约束。

2.5　互联网络下的通信保密体系结构

一直以来,有关互联网安全的技术多指密码学,使用密码学可以将在互联网络中传输的报文变成安全的、能够抵抗一定攻击的技术,能够解决互联网中的信息安全问题,如保密性、完整性、鉴别性和不可否认性。

但随着科技的进一步发展,传统数据报文保密的手段已经无法完全保障互联网中传输信息的安全性,于是越来越多的学者设法引入信息隐藏技术进一步保障数据的安全性。

2.5.1　网络即时通信系统的体系结构

图 2-7 为一般情况下的一个即时通信体系架构。

即时通信系统涉及许多方面,如服务器架构、数据库搭建、软件通信协议、数据控制以及存储等,而建立在不同开发平台上的即时通信软件可能会采用不同的体系架构。

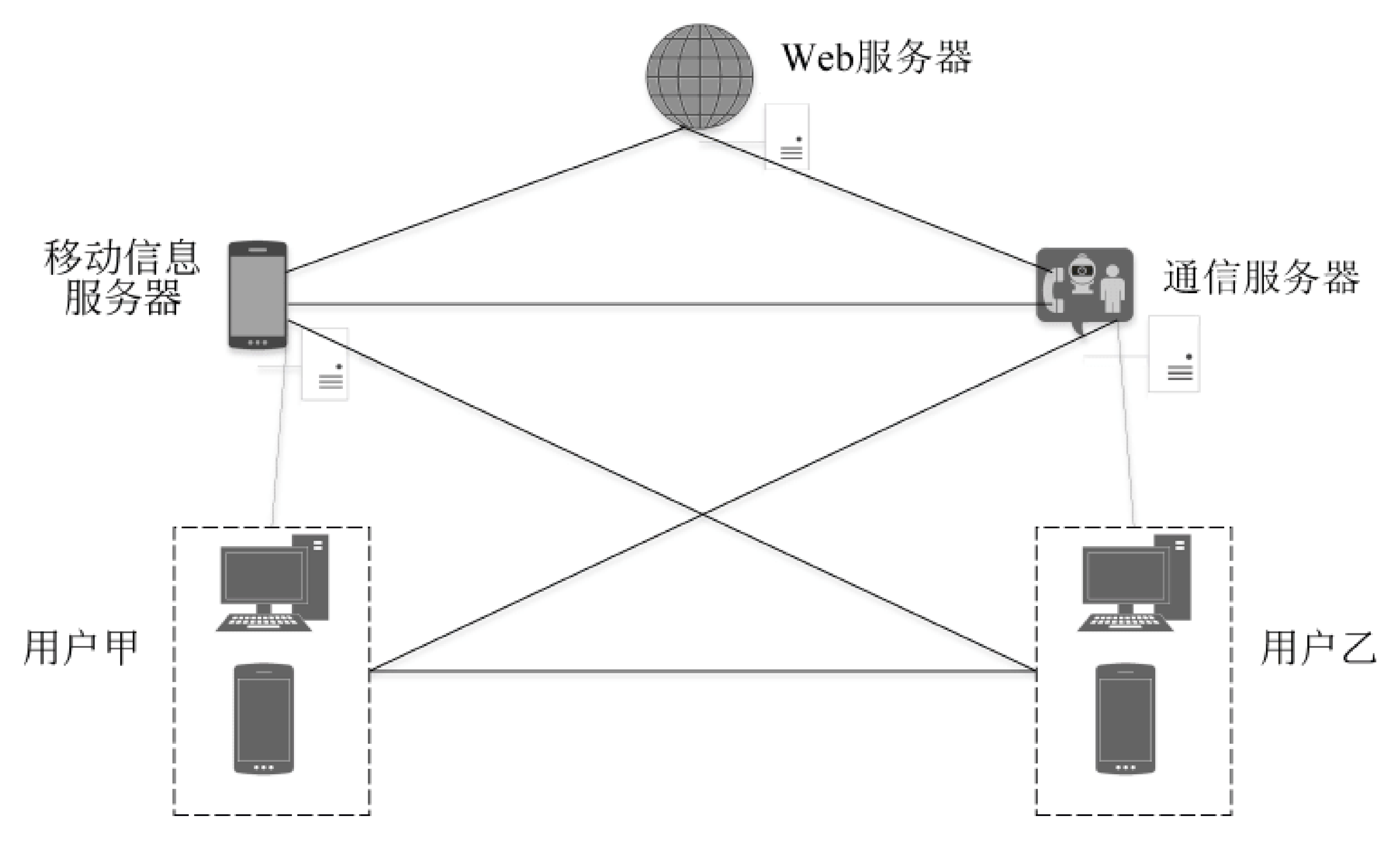


图 2-7　即时通信体系架构

2.5.2　即时通信系统的传输模式

即时通信技术是一种基于互联网的通信技术，涉及的领域非常广泛，主要包括 IP、TCP、UDP、RMTP 等网络协议，以及 P2P 技术、多媒体编解码技术等。根据应用背景的不同，即时通信技术可使用多种通信模式。

C/S 模式：以至少一个服务器或服务器集群为中心，客户端先与服务器建立连接后才能进行通信。在 C/S 架构模式下，由于客户端数量众多并且每个客户端都是并发访问，因此服务器采用分层结构进行并发控制。

P2P 模式：另一种即时通信模式。与 C/S 模式不同，P2P 模式属于对等通信模式，不存在中心结点。每个客户端都是对等的通信实体，在使用服务的同时也在提供服务。P2P 通信模式下通常存在一个服务器用于协助客户端之间建立 P2P 连接，连接建立成功后，通信双方客户端之间就可以脱离服务器使用 P2P 信道进行通信了。

混合模式：在即时通信系统中，一般采用 C/S 和 P2P 相结合的通信模式，如图 2-8 所示。C/S 模式为用户提供了身份认证、客户机状态管理等功能。P2P 模式负责为用户提供客户机之间的通信功能，两种模式相互结合，以提高系统性能和通信效率。

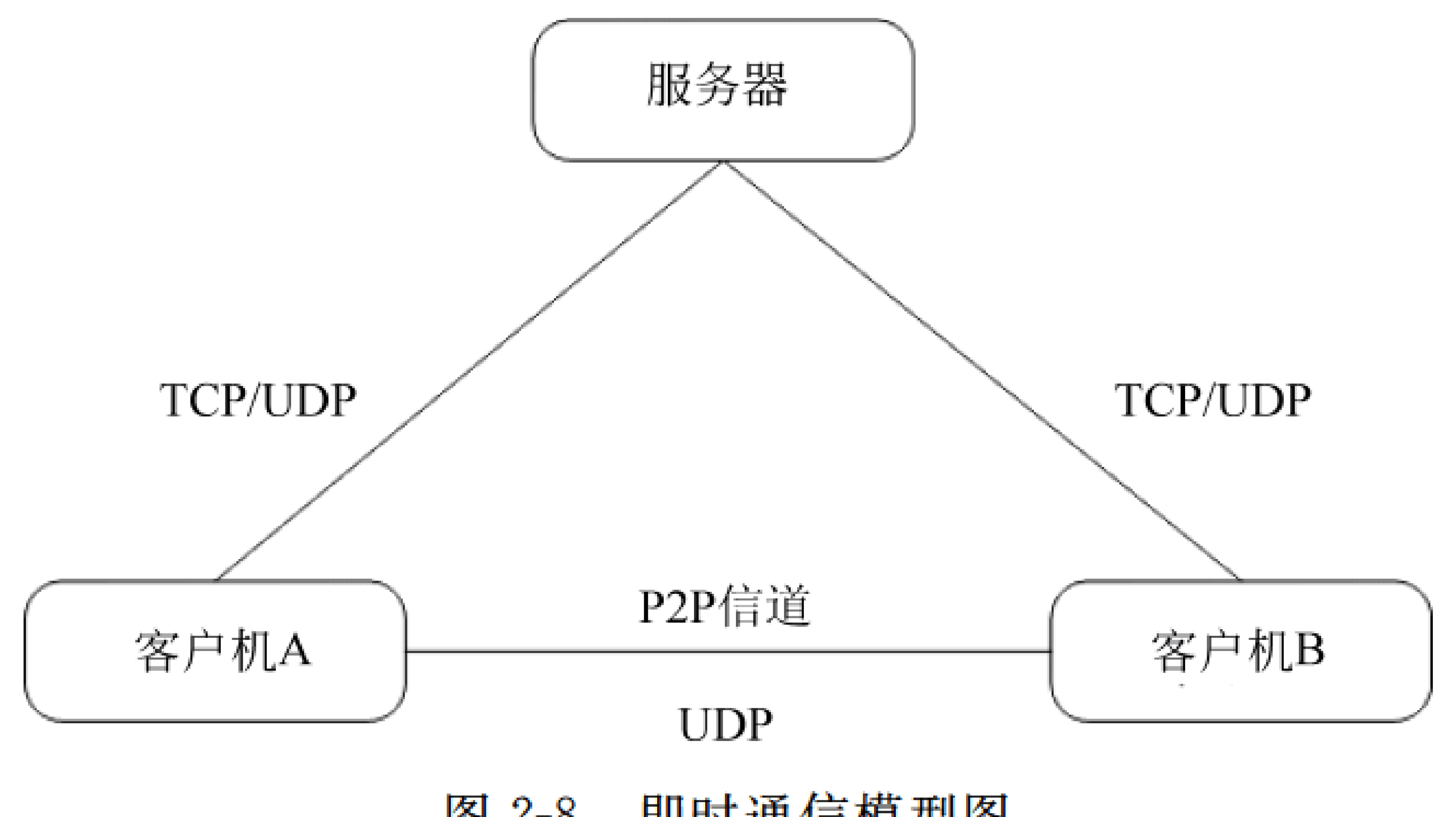


图 2-8　即时通信模型图

2.5.3 网络终端的保密应用系统

在应用层，开发终端的保密应用系统主要是为网络客户端提供一个安全的服务介入。除正常的即时通信功能外，用户还可以借用应用系统提供的诸如加密以及隐密等技术对敏感的数据内容进行在线或下线的保护。

第 3 章 水印认证码

将水印看作一种通信系统加以研究，从信息论的角度对水印的嵌入容量、失真以及噪声信道下认证码的概念等进行分析。在该研究方向上，国内外比较突出的学者主要有 P. Moulin、J. A. O'sullivan、R. Ahlswede、G. Dueck 和蔡宁等人。本章主要对上述学者的研究成果进行了分析和总结。从信息论的角度研究水印问题所建立的研究模型以及方法思路也是后续应用的理论基础。

3.1 相关定义

定理 3.1 令 V 表示一个有限的字符集，v 是取值在集合 V 中的随机变量。于是可假定掩饰载体由一无记忆具有变量 V 属性的信源 $\{V^n|_{n=1}^{\infty}\}$ 产生。密信 m 则独立于载体从一个有限集合$\{1,2,\cdots,M\}$中均匀地选取。编码者可根据信源输出的原始载体 u^n 和密信 m，编码输出一个与载体序列长度相同的序列 $x^n(=x^n(u^n,m))$（注意：这里假设信源输出的消息序列的长度和经编码后的码长度相同，同为 n）。

定理 3.2 为了测定中间过程（水印信道）的失真，引入一个累计类型的失真测度 ρ，因此，对于任意两个序列变量 $\boldsymbol{u}^n=(u_1,u_2,\cdots,u_n)\in V^n$，$\boldsymbol{x}^n=(x_1,x_2,\cdots,x_n)\in X^n$，都有

$$\rho(u^n,x^n)=\frac{1}{n}\sum_{t=1}^{n}\rho(u_t,x_t) \tag{3-1}$$

由式(3-1)可以看出，$\rho(u^n,x^n)$ 为平均失真率。

定理 3.3 攻击者使用单一的离散无记忆信道 W 攻击水印序列 x^n，攻击信道的输入为 x^n，输出为 y^n。为了便于记述方便，期间假设他们分别从有限的字符集合 V、X 和 Y 中而来。

注意，对于攻击信道的输出也必须加以失真约束。不失一般性，假定单一无记忆攻击信道自动满足失真约束条件。

定理 3.4 为了安全，约定在发送端的编码器通常通过一个编码映射置乱掩饰文本，而在接收端的解码器需要一个逆映射的过程恢复密信。

定理 3.5 边信息（Side Information）和认证 Key：基于建立为编码器及解码器分享的密钥源（Key-Resources）的考虑，将水印认证码同具有边信息的水印认证码（WIDCSI），以及具有安全 Key 的水印认证码（WIDCK）在概念上加以区分。

定理 3.6 WIDCSI：在参考文献[2]中 WIDCSI 被称为一个“在发送者和接收者之间具有边信息的水印认证编码”。

假设在时间 t，编码器能够根据掩饰文本的现时输出 $L_t = l_t$ 以及以给定的条件概率 $P_{L/V}(\cdot \mid u)$ 产生"某个 Key 的成分"。这就是说，如果源输出一个掩饰文本 u^n 的序列，编码器则以概率 $P^n_{L/V}(l^n \mid u^n)$ 输出产生一个联合概率条件下的序列 $L^n = (L_1, L_2 \cdots, L_n) = l_n = (l_1, l_2 \cdots, l_n)$，而且发送者将它发送到接收端的解码器。后者则试图借助边信息 $L^n = l^n$ 从攻击无效的消息中恢复出水印。

这种情况下，依赖于 Key 的信源事实上是由条件分布 $P_{L/V}$ 决定或者等效于联合分布概率 P_{LV}。因此，这可理解为在编码器和解码器两边是纯粹的边信息，而不是"安全的 Key"。那就是说，如果 $\{V^n|_{n=1}^{\infty}\}$ 是具有一般 V 属性的一个无记忆的掩饰文本，而且 $\{L^n|_{n=1}^{\infty}\}$ 为能被编码器和解码器随时观察到的边信息，于是 $\{(v^n, l^n)\}$ 就是具有一般 $[V, L]$ 属性的相关无记忆源。因此，解码器能够从边信息中学习到有关掩饰文本的某些特征信息，而对于攻击者什么也不知道。这种假设的根本原因是：作为通信双方，Alice 和 Bob 始终拥有比 Oscar 多得多的背景知识！

于是，一个 $(n, R, \lambda_1, \lambda_2, D_1)$ WIDCSI 就是一个对于 $m = \{1, 2, \cdots, M\}$，满足以下条件 $\{Q_m, D_m(l^n): l^n \in L^n, m \in M\}$ 的系统。

Q_m：混沌映射矩阵。

对于所有 $m = 1, 2, \cdots, M, Q_m: V^n \times L^n \to X^n$，都有

$$\sum_{u^n \in V^n, l^n \in L^n} P^n_{VL}(u^n, l^n) \sum_{x^n \in X^n} Q_m(x^n \mid u^n, l^n) \rho(u^n, x^n) \leqslant D_1 \tag{3-2}$$

这里，P_{VL} 表示一般的 (V, L) 的联合分布。

D_m：与 Q_m 相反且互逆的映射矩阵。

对于所有的 $l^n \in L^n, m \in M, D_m$：$D_m(l^n) \subset Y^n$，都有

$$\sum_{u^n \in V^n, l^n \in L^n} P^n_{VL}(u^n, l^n) \sum_{x^n \in X^n} Q_m(x^n | u^n, l^n) W^n(D_m(l^n) | x^n) > 1 - \lambda_1 \tag{3-3}$$

这里，λ_1 表示第一类型错误。

而且对于所有 $m, m' \in M, m \neq m'$，

$$\sum_{u^n \in V^n, l^n \in L^n} P^n_{VL}(u^n, l^n) \sum_{x^n \in X^n} Q_m(x^n | u^n, l^n) W^n(D_{m'}(l^n) | x^n) < \lambda_2 \tag{3-4}$$

这里，λ_2 表示第二类型错误。

码率的定义为

$$R = \log\log | M | \tag{3-5}$$

定理 3.7 WIDCK：假设编码器能够根据整个随机掩饰文本 $V^n = u^n$ 的输出，以任意方式产生一个 Key：$K_n = K_n(u^n)$，而且将之通过一个安全(无噪声)信道发送到解码器。因此，攻击者绝对不知道载体(除了分布)，也不知道 Key。因为对于掩饰文本 u^n 的一个给定输出，编码器也许会随机产生一个 K_n，由此可认为 WIDCSI 码是一种特殊的 WIDCK 编码，通常情况下后者更加有效。

注意，掩饰文本输出确定的 Key 是由一特殊的 Key 函数确定的。当然，Key 的大小必须加以限制，我们要求它随着编码长度的增加而按指数规律增加，而且在码率上受限于 Key 率 R_K。当 R_K 大于掩饰文本的熵 $H(V)$，编码器自然能够通知解码器掩饰文本的输出。但是，Key 的"剩余部分"也许会看成是增加认证容量的通信者之间的随机性

冗余[3,4,7]。

于是，一个 $(n,R,R_K,\lambda_1,\lambda_2,D_1)$ WIDCK 码为：对于所有 $M=\{1,2,\cdots,M\}$，满足以下条件 $\{Q_m^*,D_m^*(k_n),W_{K_n}: m\in M,k_n\in K_n\}$ 的系统。

$Q_m^*, m=1,2,\cdots,M$ 是从 $V^n\times K_n\to X^n$ 的混沌映射矩阵(攻击信道输入的字符)，这样

$$\sum_{u^n\in V^n}P_V^n(u^n)\sum_{k_n\in K_n}W_{K_n}(k_n|u^n)\sum_{x^n\in X^n}Q_m^*(x^n|u^n,k_n)\rho(u^n,x^n)\leqslant D_1 \tag{3-6}$$

对于所有 $k_n\in K_n, m\in M, D_m(k_n)\subset y^n$，第一类型错误。

$$\sum_{u^n\in V^n}P_V^n(u^n)\sum_{k_n\in K_n}W_{K_n}(k_n|u^n)\sum_{x^n\in X^n}Q_m^*(x^n|u^n,k_n)W^n(D_m(k_n)|x^n)>1-\lambda_1 \tag{3-7}$$

对于所有的 m，$m'\in M$，$m\neq m'$，第二类型错误。

$$\sum_{u^n\in V^n}P_V^n(u^n)\sum_{k_n\in K_n}W_{K_n}(k_n|u^n)\sum_{x^n\in X^n}Q_m^*(x^n|u^n,k_n)W^n(D_{m'}(k_n)|x^n)>\lambda_2 \tag{3-8}$$

码率的定义见式(3-5)。

K_n 是一有限域上的集合，将被称为密钥书，而且

$$\frac{1}{n}\log|K_n|\leqslant R_K \tag{3-9}$$

R_K 称为 Key 率。

W_{K_n} 是一个混沌映射矩阵 $W_{K_n}: V^n\to K_n$。当掩饰文本 V_n 被随机输入到信道 W_{K_n} 中，其输出的随机变量将被记为 K_n。也就是说，随机变量对 (V^n,K_n) 具有联合概率分布：$P_{V^nK^n}(u^n,k^n)=P_V^n(u^n)W_{K_n}(k_n\mid u^n), u^n\in V, k_n\in K_n$。

特殊地，K^n 也许是掩饰文本输出的确定的函数，而且在 $P_{V^nK^n}(u^n,k^n)=P_V^n(u^n)W_{K_n}(k_n\mid u^n)$ 的情况下，我们将 K^n 写成定义在 V^n 上的函数(注意，K^n 的选取不依赖于消息 $m\in M$，因为 Key 将不依赖于所保护的消息)。

定理 3.8 信道容量：两种类型的编码容量分别记为 $C_{WIDSI}((V,L),W,D_1)$ 以及 $C_{WIDK}((V,W),R_K,D_1)$，(V,L) 和 L 分别是通常意义下的无记忆相关源以及源；W 是一无记忆攻击信道；P_K 是 Key 率，而 Δ_1 是失真判据。

3.2 相关信源模型

分享一定公用信源的两者(或多者)之间的随机性，也许是相关的信源，或者是特指(有噪声或无噪声)的一些信道。这些两者之间的随机性仅仅是公共域上的两个随机变量，相互之间在概率上是收敛的。可以根据信源的情况建立不同的模型。

处于建立水印认证码的目的，我们需要随机性的两种类型。下面，相关源 $\{(V_n,L_n)\}_{n=1}^{\infty}$ 对应于掩饰文本以及边信息，而无记忆信道 W 对应于在水印认证中的攻击信道。模型Ⅱ中的 K_n 对应于 WIDCK 的模型。

3.2.1 模型Ⅰ：具有两个源的约束噪声信道

令 $\{(V_n,L_n)\}_{n=1}^{\infty}$ 是分别具有两个分量 V 和 L 的相关无记忆源，字符集 V 和 L 类属

(V,L)。假设有两个人,如发送者和接收者。发送者可能能观测到整个源 (V_n,L_n) 的整个输出,而接收者只能观测到分量 L_n。

基于以上考虑,发送者为了建立公共随机性,在一定的约束条件下,可以通过无记忆信道 W 向接收者发送消息,而接收者则规定不允许向发送者发送任何消息。W 信道的输入取自字符集 X,输出则属于字符集 Y。

发送者首先从码字集合 $u \in x^n$ 中选择一个具有长度为 n 的源输出序列作为信道码字,同时产生一个随机变量 M,M 代表他/她在一有限集合 M 上均匀取值的"私有的随机数",而且与源输出 (V_n,L_n) 相互独立。

假设给定一个在式(3-1)中定义的失真测度 ρ 和一个失真判据 D_1。根据源输出 $(V_n,l_n)=(u_n,l_n)$ 以及私有的随机数 $M=m$,发送者选择一编码字 $x_m(u^n,l^n)\in u(\subset x^n)$,使编码字和相关源 $V^n=u^n$ 的分量之间的失真也不会超出 D_1。也就是说,

$$\frac{1}{n}\sum_{m\in M}P_M(m)\sum_{u^n\in V^n}\sum_{l^n\in L^n}P_{VL}(u^n,l^n)\rho(x_m(u^n,l^n),u^n)\leqslant D_1 \tag{3-10}$$

如果发送者给信道输入码字 $x_m(u^n,l^n)$,接收者则以概率 $W^n(y^n\mid x_m(u^n,l^n))$ 收到一个序列 $y^n\in Y^n$,我们还可以选择 $x_m(u,l^n)$ 为随机输入序列而替代一个确定的序列(这在证明上是方便的)。

最后,对于一个有限集合 A,其长度典型地随着源输出长度 n 的增加而指数增加。也就是说,存在一个常数 k,

$$\frac{1}{n}\log|A|\leqslant k, \tag{3-11}$$

发送者依据信源的输出 (V^n,L^n) 和 M,通过一个函数创建一个在支撑域 A 上的随机映射变量 F,

$$F: V^n\times L^n\times M\to A \tag{3-12}$$

而接收者根据信道 W^n 的输出和信源分量 L^n 的输出,通过一个函数创建一个随机逆映射变量 G,

$$G: L^n\times Y^n\to A \tag{3-13}$$

根据文献[3]中的术语,我们称由上述方法得出的随机变量对(F,G)是可达的,并且称(F,G)是一种 λ-类型的公用随机对。如果

$$Pr\{F\neq G\}<\lambda \tag{3-14}$$

典型地,当源序列长度 n 足够大时,λ 可以是一任意小的正实数。如果式(3-14)中的 λ 任意小,不难看出在式(3-11)和式(3-14)条件下,由 Fano 不等式可得熵率 $\frac{1}{n}H(F)$ 和 $\frac{1}{n}H(G)$ 可以任意接近,这一点从文献[3]也能看出。因此,我们选择 $\frac{1}{n}H(F)$ 和 $\frac{1}{n}H(G)$ 的其中之一作为随机数的熵率。

定义:如果对于任意正实数和足够大的 n(依赖于 ε、λ 和 μ),都存在一个 λ-型的公共随机数满足式(3-10)~式(3-14)。并且

$$C_{\mathrm{CRII}}((V,L),W,R_K,D_1)\leqslant\inf_{W\in W(V,L,U,X,Y)}\max_{\in Q*((V,L),W,R_K,D_1)}[I(U;L,Y)+H(L\mid U)]+R_K$$

我们称一数对 (r,D_1) 为公共随机可达的，于是有

$$\frac{1}{n}H(F)>r-\varepsilon \tag{3-15}$$

以及

$$\sum_{a\in A}Pr\{F=a\}-\frac{1}{A}<\mu \tag{3-16}$$

最后一个条件式(3-16)要求公共随机概率必须是近似平均分布，并且称为近似均匀条件，这样要求是为了减少认证码的第二类错误。可达数对的集合称为公共随机概率的容量范围。对于固定的 D_1，一般随机概率的容量定义为

$$C_{CRI}((V,L),W,D_1)=\max\{r:(r,D_1)\} \tag{3-17}$$

注意，在当前模型和下一个模型Ⅱ中，发送者的个人随机数并没有加以限制，这是因为实际信道的容量是有限的。

这个模型和文献[3]中的模型Ⅰ有三点不同。

第一，在文献[3]的模型Ⅰ中，发送者和接收者之间的信道速率是小于或等于 R 的无噪信道，而当前模型一般是有噪声的。

第二，本模型对信源失真度的要求不仅扮演边信息的角色，还扮演限制者的角色。也就是说，为了减少失真，发送者必须选择适当的码字，这使得变换更加困难。为了说明这一点，考虑一个极端的状况：信源的边信息是一个常量，在模型Ⅰ中，信源完全没有影响，因此一般随机容量等于信道容量。而在本模型中信道起作用，因为发送者可能不会自由地选择码字，因此减少了一般随机性，获得本模型的容量范围也是绝对非平凡的。

第三，在本模型中，发送者和接收者分别观察序列 $(V^n,L^n)=(u^n,l^n)$ 和 $L^n=l^n$。在转换之前，一般随机概率的熵 $H(L^n)=I(V^n,L^n;L^n)$（两个观测者之间的互信息）。因此，并不奇怪定理 $C_{CRI}((V,L),W,D)=\max\limits_{(V,L,U,X,Y)\in Q((V,L),W,D)}[I(U;L,Y)+H(L\mid U)]$ 和文献[3]中的定理不同，该定理不能简单地通过将无躁信道的速率替换为有噪信道的容量获得。

3.2.2 模型Ⅱ：双源的带约束噪声信道和无噪声信道

很明显，研究模型Ⅰ的目的是为了构建带边信息的水印认证码 WIDCSI。接下来，为了研究带密钥的水印认证码 WIDCK，引入一般随机性的模型Ⅱ。实际上，我们增加了所谓的“边信息”，导致建立的模型比实际需要的模型更具有一般性。于是，为了定义模型Ⅱ，只要在模型Ⅰ的基础上再增加一条无噪声信道，而为此几乎不需要增加额外的工作。

也就是说，我们假定相关信源为 $\{(V^n,L^n)\}_{n=1}^{\infty}$、有噪信道 W、失真约束式(3-10)和发送者的个人随机 M 依然有效。另外，发送者从消息集合 K_n 中选择一条消息 k_n 以速率 $\frac{1}{n}\log|K|\leqslant R_K$ 通过一无噪信道发送给接收者。当然，k_n 必须是信源输出和发送者个人随机数（水印）的函数，即

对于 $u^n\in V^n,m\in M,k_n=K_n(u^n,m)$，更一般的情况是，发送者采用随机策略，将 k_n 看作输入为 (u^n,m) 的攻击信道 $(W\mid K)$ 的输出。为了定义此模型的一般随机性，将式

(3-13)修改为

$$G: K_n \times L^n \times Y^n \rightarrow A \tag{3-18}$$

同时保持式(3-10)～式(3-16)不变。

类似地，也可以定义 $C_{CRII}((V,L),W,R_K,D_1)$、相关无记忆信源 (V,L)、无记忆信道 W、Key 率 P_k 以及失真测度 D_1。

3.2.3 模型Ⅲ：复合信道

假设攻击者从一簇满足攻击失真标准的信道中选择一条平稳无记忆的信道攻击水印，而编码者和解码者都不知道攻击者选用的是哪一条信道，这些信道在信息论中被称为复合信道。这种假设比文献[6]中解码者在已知攻击信道的前提下解码的假设更鲁棒一些。事实上，该假设应该是最严苛的假设。

定理 3.9 一个复合信道是一簇输入输出字母表分别为 X 和 Y 的无记忆信道 $W=\{(\cdot|\cdot,s): s \in S\}$，$\Sigma$ 为状态集，信道输出概率

$$W^n(y^n \mid x^n, s) = \prod_{t=1}^{n} W(y_t \mid x_t, s) \tag{3-19}$$

这里，信道由状态 s 控制，输入为 $x^n \in X^n$。

假设攻击者在知道编码的分布 P_n 的前提下使用复合信道攻击水印传输或认证码，他会选择这样一条复合信道，对所有的 $s \in \Sigma$，

$$\frac{1}{n}\sum_{x^n \in X^n} P_n(x^n) \sum_{y^n \in Y^n} W_n(y^n \mid x^n, s)\rho'(x^n, y^n) \leqslant D_2 \tag{3-20}$$

这里，ρ' 是一个加性失真度量，被称为攻击失真度。它和水印失真度 ρ 可能一样，也可能不一样，D_2 是攻击失真标准。特别地，当编码字由一个具有独立同分布性质的输入产生，那么由编码字导致的输入也为独立同分布。

$$P^n(x^n) = \prod_{t=1}^{n} P(x_t) \tag{3-21}$$

这样，复合信道对于所有 $s \in \Sigma$，

$$\sum_{x \in X^n} P(x) \sum_{y \in Y^n} W(y \mid x, s)\rho'(x, y) \leqslant D_2 \tag{3-22}$$

也许是成立的。不过，通常假设在一定前提下的所有复合信道都满足以上失真条件。

对于复合信道的 WIDCSI 码：通过替换式(3-3)和式(3-4)中对所有 $l^n \in L^n, m \in M$，$D_m(l^n) \in Y^n$，以及 $s \in S$，分别为

$$\sum_{u^n \in V^n, l^n \in L^n} P_{VL}^n(u^n, l^n) \sum_{x^n \in X^n} Q_m(x^n \mid u^n, l^n) W^n(D_m(l^n) \mid x^n, s) > 1 - \lambda_1 \tag{3-23}$$

以及，对所有 $m, m' \in M, m \neq m'$，$s \in S$，

$$\sum_{u^n \in V^n, l^n \in L^n} P_{VL}^n(u^n, l^n) \sum_{x^n \in X^n} Q_m(x^n \mid u^n, l^n) W^n(D_{m'}(l^n) \mid x^n, s) < \lambda_2 \tag{3-24}$$

对于 WIDCK 复合信道：通过替换式(3-7)和式(3-8)中对所有 $l^n \in L^n, m \in M, D_m(k_n) \subset Y_n$，以及 $s \in S$，分别为

$$\sum_{u^n \in V^n} P_V^n(u^n) \sum_{k^n \in K^n} W_{K_n}(k_n|u^n) \sum_{x^n \in X^n} Q_m^*(x^n|u^n, k_n) W^n(D_m(k_n)|x^n, s) > 1 - \lambda_1 \tag{3-25}$$

以及对所有 $m, m' \in M, m \neq m'$，

$$\sum_{u^n \in V^n} P_V^n(u^n) \sum_{k^n \in K^n} W_{K_n}(k_n|u^n) \sum_{x^n \in X^n} Q_m^*(x^n|u^n,k^n) W^n(D_{m'}(k_n)|x^n,s) < \lambda_2 \quad (3\text{-}26)$$

这里，Q_m、Q_m^*、$D_m(l^n)$ 以及 $D_m(k_n)$ 和决定信道的状态是独立不相关的。这反映了编码器和解码器均不能知道信道状态的要求，而且之所以式(3-18)～式(3-21)对所有 $s \in S$ 成立，是因为考虑的编码器和解码器总是面对最坏的情况。

式(3-18)以及式(3-20)表明，当遍历所有 M 和 S 态，正确检测率必大于 $1-\lambda_1$。式(3-17)和式(3-21)表明：误检率必小于 λ_2。当 λ_1、λ_2 分别趋近于 0，表明解码器检测成功概率接近于 1，错误概率接近于 0。

至于模型Ⅰ和模型Ⅱ中的一般随机性：对复合信道，可替换式(3-14)为：在任何状态 s 控制下的信道，

$$Pr\{F \neq G \mid s\} < \lambda \quad (3\text{-}27)$$

此外，因为不知道编码器和解码器状态，因此函数 F、G 以及编码字是独立于状态 s 的。类似地，对于复合信道 W，相应的水印认证码的容量和一般随机性下的认证码可分别表示为

$C_{\text{WIDSI}}((V,L),W,D_1)$、$C_{\text{WIDK}}(V,W,R_K,D_1)$、$C_{\text{CRI}}((V,L),W,D_1)$ 以及 $C_{\text{CRII}}((V,L),W,R_K,D_1)$。

3.3 一般随机性的研究结论

对一个给定的相关的无记忆信源 $\{(V^n,L^n)\}_{n=1}^{\infty}$，它的联合概率分布为 P_{VL}，若无记忆信源为 W，失真标准为 D_1，$Q((V,L),W,D_1)$ 代表一个域为 $V\times L\times U\times X\times Y$ 且具有如下性质的随机变量的集合，这里 U 是一个有限集且其基数满足 $|U| \leqslant |V||L||X|$；X、Y 分别是信道 W 的输入输出字母表。

对于所有 $v \in V, l \in L, u \in U, x \in X$ 以及 $y \in Y$，

$$\begin{aligned} Pr\{(V,L,U,X,Y)=(v,l,u,x,y)\} &= P_{\text{VLUXY}}(v,l,u,x,y) \\ &= P_{\text{VL}}(v,l)P_{\text{UX|VL}}(u,x \mid v,l)W(y \mid x) \end{aligned} \quad (3\text{-}28)$$

对于给定的失真度 ρ

$$E\rho(V,X) \leqslant D_1 \quad (3\text{-}29)$$

$$I(U;V,L) \leqslant I(U;L,Y) \quad (3\text{-}30)$$

于是，我们在模型Ⅰ中针对单一信道 W 获得随机性编码定理如下。

定理 3.10 模型Ⅰ含有边信息的在约束条件 D_1 下的攻击信道的容量为

$$C_{\text{CRI}}((V,L),W,D_1) = \max_{(V,L,U,X,Y)\in Q((V,L),W,D_1)} [I(U;L,Y)+H(L \mid U)] \quad (3\text{-}31)$$

对于一给定具有一般 (V,L) 联合分布的相关源、信道 W、正实数 R_K 以及判据 D_1，用 $Q^*((V,L),W,R_K,D_1)$ 记为随机变量集合 (V,L,U,X,Y) 的分布，而且和上面定义的支撑域相同。这样，式(3-28)、式(3-29)以及

$$I(U;V,L) \leqslant I(U;L,Y) + R_K \tag{3-32}$$

都成立。

定理 3.11 模型Ⅱ含有 Key 的边信息，在约束条件 D_1 下的攻击信道的容量为

$$C_{\mathrm{CRII}}((V,L),W,R_K,D_1) = \max_{(V,L,U,X,Y)\in Q^*((V,L),W,R_K,D_1)} [I(U;L,Y) + H(L \mid U)] + R_K \tag{3-33}$$

为了描述复合信道的编码理论，需要重新定义符号。如同上面一样，对于具有 $V \times L \times U \times X$ 字符集的随机变量 (V,L,U,X)，分别看成输入 X 和输出 Y 的信道，记作 $Y(W)$。这样，联合分布 $P_{LVUXY(W)} = P_{LVUX}(W)$，$LVU \leftrightarrow X \leftrightarrow Y$ 构成一马尔可夫链。

对于具有状态集 $S(s \in S)$，复合信道 W 仍然记为 $Y(W(\cdot \mid \cdot, s)) = Y(s)$。可以重新定义如下：

$$I(U;L,Y(W)) = \inf_{s\in S} I(U;L,Y(s))$$

和

$$I(U;Y(W) \mid L) = \inf_{s\in S} I(U;Y(s)L)$$

为了方便，当用 $P_{\tilde{L}\tilde{V}\tilde{U}\tilde{X}}$ 代替 P_{LVUX} 时，也记 $Y(s)$ 为 $\widetilde{Y}(s)$。

$$I(U;L,Y(W)) = I(U;L) + I(U;Y(W) \mid L) \tag{3-34}$$

现在，对于复合信道，我们定义 $Q_1((V,L),W,D_1)$ 为随机变量 (V,L,U,X) 的集合。这样，对于前两个分量的边缘分布等于分布 P_{VL}，并且式(3-29)和

$$I(U;V,L) \leqslant I(U;L,Y(W)) \tag{3-35}$$

都成立。

类似地，为了构建 $Q^*((V,L),W,R_K,D_1)$，定义 $Q_1^*((V,L),W,R_K,D_1)$ 为随机变量 (V,L,U,X) 的集合。这样，对于前两个分量的边缘分布等于 P_{VL} 分布，并且式(3-29)和

$$I(U;V,L) \leqslant I(U;L,Y(W)) + R_K \tag{3-36}$$

都成立，则有定理 3.12 和定理 3.13。

定理 3.12

$$\begin{aligned}
&\sup_{(V,L,U,X)\in Q_1(V,L),W,D_1} [I(U;L,Y(W)) + H(L \mid U)] \\
&\leqslant C_{CRI}((V,L),W,D_1) \\
&\leqslant \inf_{W\in w} \max_{(V,L,U,X,Y)\in Q((V,L),W,D_1)} [I(U;L,Y) + H(L \mid U)]
\end{aligned} \tag{3-37}$$

定理 3.13

$$\begin{aligned}
&\sup_{(V,L,U,X)\in Q_1^*(V,L),W,R_K,D_1} [I(U;L,Y(W)) + H(L \mid U)] + R_K \\
&\leqslant C_{CRII}((V,L),W,R_K,D_1) \\
&\leqslant \inf_{W\in w} \max_{(V,L,U,X,Y)\in Q^*((V,L),W,R_K,D_1)} [I(U;L,Y) + H(L \mid U)] + R_K
\end{aligned} \tag{3-38}$$

注意：定理 3.12 和定理 3.13 中的下、上界的间隙差取决于 inf-sup 的阶。

3.4 对于水印认证码的结果

对于集合 V、X、Y 以及一个具有基数 $|V||X|$ 的有限集合 U，一个具有一般 $|V|$ 的无记忆源 V，一个无记忆信道 W，以及混合信道 $Y(w)$，定义以下集合。

A. 令 $Q^{**}(V,W,R_K,D_1)$ 为具有 $(v\times u\times x\times y)$ 支撑域的随机变量 (V,U,X,Y) 的集合，对于所有 $v\in V,u\in U,x\in X,y\in Y$，

$$P_{VUXY}(v,u,x,y)=P_V(v)P_{UX|V}(u,x\mid v)W(y\mid x) \tag{3-39}$$

$$I(U;V)\leqslant I(U;Y)+R_K \tag{3-40}$$

以及式(3-29)都成立。

式(3-40)表明：有限集合 U 和无记忆信源 V 之间的互信息小于 U 和信道输出 Y 之间的互信息以及 Key 率之和。可以这样理解：如果没有 R_K 这一项，且 $X\rightarrow Y$ 是线性系统的情况下，则可以认为等号成立。

B. 令 $Q_1^*(V,W,R_K,D_1)$ 为具有支撑域 $v\times u\times x$ 的随机变量 (V,U,X) 的集合。于是，对于所有 $v\in V,u\in U,x\in X$，

$$P_{VUX}(v,u,x)=P_V(v)P_{UX|V}(u.x\mid v) \tag{3-41}$$

$$I(U;V)\leqslant I(U;Y(w))+R_K \tag{3-42}$$

以及式(3-29)成立。这里，$I(U;Y(w))=\inf\limits_{W\in w}I(U;Y(W))$。

特别地，当相关源对 $\{(V^n,L^n)\}_{n=1}^{\infty}$ 中的第二个分量 L^n 是一个常数时，$Q^*((V,L),W,R_K,D_1)$ 以及 $Q_1^*((V,L),w,R_K,D_1)$ 分别变成 $Q^{**}(V,W,R_K,D_1)$ 和 $Q_1^{**}(V,w,R_K,D_1)$。

定理 3.14

$$C_{WIDSI}((V,L),W,D_1)\geqslant\max_{(V,L,U,X,Y)\in Q((V,L),W,D_1)}[I(U;L,Y)+H(L\mid U)] \tag{3-43}$$

定理 3.15

$$C_{WIDK}(V,W,R_K,D_1)\geqslant\max_{(V,U,X,Y)\in Q^{**}(V,W,R_K,D_1)}[I(U;Y)+R_K \tag{3-44}$$

定理 3.16

$$C_{WIDSI}((V,L),w,D_1)\geqslant\max_{(V,L,U,X)\in Q_1((V,L),w,D_1)}[I(U;L,Y(w))+H(L\mid U)] \tag{3-45}$$

定理 3.17

$$C_{WIDK}(V,W,R_K)\geqslant\max_{(V,U,X)\in Q_1^{**}(V,w,R_K,D_1)}[I(U;Y(w))+R_K \tag{3-46}$$

注意，在定理 3.14 和定理 3.16 中可以加入相关源的第二个分量 L^n 的边信息，于是可以获得相应的较小的界，而证明过程几乎不变。

定理 3.18(均匀覆盖) 对于 $l^n\in T_{\tilde{L}}^n,U_i(l^n)i=1,2,\cdots,\lfloor 2^{na}\rfloor$是一个独立随机变量序列，分布均匀的 $T_{\tilde{U}|\tilde{L}}^n(l^n)$，对于 $T_{\tilde{U}|\tilde{L}}^n(l^n)$，让$\hat{U}_{\tilde{U}|\tilde{V}\tilde{L}}(v^nl^n)$ 成为 $\{U_i(l^n):i=1,2,\cdots,\lfloor 2^{na}\rfloor\}\cap T_{\tilde{U}|\tilde{V}\tilde{L}}^n(v^nl^n)$ 的随机集。

对于全部 $\varepsilon\in(0,1]$

$$Pr\left\{\left|\,|\hat{u}_{\tilde{U}|\tilde{V}\tilde{L}}(v^n l^n)| - \lfloor 2^{n\alpha}\rfloor \frac{|T^n_{\tilde{U}|\tilde{V}\tilde{L}}(v^n l^n)|}{|T^n_{\tilde{U}|\tilde{L}}(l^n)|}\right| \geqslant \lfloor 2^{n\alpha}\rfloor \frac{|T^n_{\tilde{U}|\tilde{V}\tilde{L}}(v^n l^n)|}{|T^n_{\tilde{U}|\tilde{L}}(l^n)|}\varepsilon\right\} < 4\cdot 2^{-\frac{\varepsilon^2}{4}2n\eta}$$

如果 n 足够大

$$\lfloor 2^{n\alpha}\rfloor > 2^{n\eta}\frac{|T^n_{\tilde{U}|\tilde{L}}(l^n)|}{|T^n_{\tilde{U}|\tilde{V}\tilde{L}}(v^n l^n)|}$$

定理 3.19 对于 n 型 $P_{\tilde{L}\tilde{U}}$，$U_i(l^n)$，$i=1,2,\cdots,\lfloor 2^{n\alpha}\rfloor$ 是一个均匀分布的独立随机变量序列。设 y 为有限集，对于所有 n 型 $P_{\tilde{L}\tilde{U}\tilde{Y}}$ 和具有公共边际分布 $P_{\tilde{L}\tilde{U}}$ 性质的 $P_{\tilde{L}\tilde{U}\tilde{Y}}$ 和 $P_{\tilde{Y}}=P_{\tilde{Y}}$，以及所有 $i,\gamma>0$ 和足够大的 n，

$$Pr\left\{\frac{1}{\lfloor 2^{n\alpha}\rfloor}\sum_{i=1}^{\lfloor 2^{n\alpha}\rfloor} T^n_{\tilde{Y}|\tilde{L}\tilde{U}}(l^n U_i(l^n)) \cap \left[\bigcup_{j\neq 1} T^n_{\tilde{Y}|\tilde{L}\tilde{U}}(l^n U_j(l^n))\right] | \geqslant t_{\tilde{Y}|\tilde{L}\tilde{U}} 2^{-\frac{n}{2}\gamma}\right\} < 2^{-\frac{n}{2}\gamma}$$

如果
$$\lfloor 2^{n\alpha}\rfloor \leqslant \frac{t_{\tilde{U}|\tilde{L}}}{t_{\tilde{U}|\tilde{L}\tilde{Y}}}2^{-n\gamma}$$

3.5 对于普通随机性的直接定理

本节证明定理 3.10～定理 3.13 的直接部分。因为一个 DMC(离散无记忆信道)可看作是一个具有单数(即 $|S|=1$) 特殊的复合信道，我们仅需证明定理 3.10～定理 3.12 的直接部分。为此，对于由变量 v、l、u 乘积为支撑域的有限集合 $v\times l\times u$ 上的 n-类型概率 $P_{\tilde{V}\tilde{L}\tilde{U}}$，需要以下 3 个引理。

引理 3.1 **均匀掩蔽**(Uniform-Packing)

对于 $l^n\in T^n_{\tilde{L}}$，令 $U_i(l^n)$，$i=1,2,\cdots,\lfloor 2^{n\alpha}\rfloor$ 是在 $T^n_{\tilde{U}|\tilde{L}}(l^n)$ 上具有独立、均匀分布的随机变化序列。且对于任意 $T^n_{\tilde{U}|\tilde{L}}(l^n)$，令 $\hat{U}_{\tilde{U}|\tilde{V}\tilde{L}}(v^n l^n)$ 为随机集合 $\{U_i(l^n): i=1,2,\cdots,\lfloor 2^{n\alpha}\rfloor\}\cap T^n_{\tilde{U}|\tilde{V}\tilde{L}}(v^n l^n)$。于是，对于所有 $\varepsilon\in(0,1]$：

$$Pr\left\{\left|\,|\hat{u}_{\tilde{U}|\tilde{V}\tilde{L}}(v^n l^n)| - \lfloor 2^{n\alpha}\rfloor \frac{|T^n_{\tilde{U}|\tilde{V}\tilde{L}}(v^n l^n)|}{|T^n_{\tilde{U}|\tilde{L}}(l^n)|}\right| \geqslant \lfloor 2^{n\alpha}\rfloor \frac{|T^n_{\tilde{U}|\tilde{V}\tilde{L}}(v^n l^n)|}{|T^n_{\tilde{U}|\tilde{L}}(l^n)|}\varepsilon\right\} < 4\cdot 2^{-\frac{\varepsilon^2}{4}2n\eta} \tag{3-47}$$

对于足够大的 n，$\lfloor 2^{n\alpha}\rfloor > 2^{n\eta}\dfrac{|T^n_{\tilde{U}|\tilde{L}}(l^n)|}{|T^n_{\tilde{U}|\tilde{V}\tilde{L}}(v^n l^n)|}$ 条件成立。

证明：令

$$Z_i(v^n,l^n)=\begin{cases}1 & U_i(l^n)\in T^n_{\tilde{U}|\tilde{V}\tilde{L}}(v^n l^n)\\ 0 & U_i(l^n)\notin T^n_{\tilde{U}|\tilde{V}\tilde{L}}(v^n l^n)\end{cases} \tag{3-48}$$

及 $q=\dfrac{|T^n_{\tilde{U}|\tilde{V}\tilde{L}}(v^n l^n)|}{|T^n_{\tilde{U}|\tilde{L}}(l^n)|}$，于是 $|\hat{u}_{\tilde{U}|\tilde{V}\tilde{L}}(v^n l^n)|=\sum_{i=1}^{\lfloor 2^{n\alpha}\rfloor} Z_i(u^n l^n)$，且对于 $i=1,2,\cdots,\lfloor 2^{n\alpha}\rfloor$，根据 $Z_i(v^n,l^n)$ 和 $U_i(l^n)$ 的定义，

$$Pr\{Z_i(v^n l^n)z\}=\begin{cases}q & z=0\\ 1-q & z\neq 0\end{cases} \tag{3-49}$$

由 Chernov 边界的定义可知，如果 $\lfloor 2^{n\alpha} \rfloor > 2^{n\eta}q^{-1}$，则

$$
\begin{aligned}
&Pr\left\{\sum_{i=1}^{\lfloor 2^{n\alpha}\rfloor} Z_i(v^n l^n) \geqslant \lfloor 2^{n\alpha} \rfloor q(1+\varepsilon)\right\} \\
&\leqslant \mathrm{e}^{-\frac{\varepsilon}{2}\lfloor 2^{n\alpha}\rfloor q(1+\varepsilon)} E\mathrm{e}^{\frac{\varepsilon}{2}\sum_{i=1}^{\lfloor 2^{n\alpha}\rfloor} Z_i(v^n l^n)} \\
&= \mathrm{e}^{-\frac{\varepsilon}{2}\lfloor 2^{n\alpha}\rfloor q(1+\varepsilon)} \prod_{i=1}^{\lfloor 2^{n\alpha}\rfloor} E\mathrm{e}^{\frac{\varepsilon}{2} Z_i(v^n l^n)} \\
&= \mathrm{e}^{-\frac{\varepsilon}{2}\lfloor 2^{n\alpha}\rfloor q(1+\varepsilon)} \left[1+(\mathrm{e}^{\frac{\varepsilon}{2}}-1)q\right]^{\lfloor 2^{n\alpha}\rfloor} \\
&\leqslant \mathrm{e}^{-\frac{\varepsilon}{2}\lfloor 2^{n\alpha}\rfloor q(1+\varepsilon)} \left[1+\left(\frac{\varepsilon}{2}+\left(\frac{\varepsilon}{2}\right)^2\right)q\right]^{\lfloor 2^{n\alpha}\rfloor} \\
&\leqslant \exp_{\mathrm{e}}\left\{-\frac{\varepsilon}{2}\lfloor 2^{n\alpha}\rfloor q(1+\varepsilon)+\frac{\varepsilon}{2}\lfloor 2^{n\alpha}\rfloor q\left(1+\frac{\varepsilon}{2}\right)\right\} \\
&= \mathrm{e}^{-\frac{\varepsilon^2}{4}\lfloor 2^{n\alpha}\rfloor q} < 2\mathrm{e}^{-\frac{\varepsilon^2}{4}2n\eta}
\end{aligned}
\tag{3-50}
$$

这里，第一个不等式遵循 Chernov 界；由式(3-49)可知第二个等式成立；第二个不等式成立，是因为 $\mathrm{e}^{\frac{\varepsilon}{2}} < 1+\frac{\varepsilon}{2}+\left(\frac{\varepsilon}{2}\right)^2$，假设 $\varepsilon < 1$，$\mathrm{e}^{\frac{\varepsilon}{2}} < \mathrm{e}^{\frac{1}{2}} < 2$；第三个不等式遵循不等式 $1+x < \mathrm{e}^x$。类似地，可以得到

$$
Pr\left\{\sum_{i=1}^{\lfloor 2^{n\alpha}\rfloor} Z_i(v^n l^n) \leqslant \lfloor 2^{n\alpha} \rfloor q(1-\varepsilon)\right\} < 2\mathrm{e}^{-\frac{\varepsilon^2}{4}2n\eta}
\tag{3-51}
$$

如果 $\lfloor 2^{n\alpha} \rfloor > 2^{n\eta}q^{-1}$。

最后，结合式(3-50)和式(3-51)，可以得到该引理的结果。

引理 3.2　填充(Packing)　令 $P_{\tilde{L}\tilde{U}}$ 为 n- 类型概率，而且 Y 是一有限域集合。对一 $l^n \in T^n_{\tilde{L}}$，假设 $U_i(l^n)$，$i=1,2,\cdots,\lfloor 2^{n\alpha} \rfloor$是一均匀分布于 $T^n_{\tilde{U}|\tilde{L}}(l^n)$ 上的独立随机变量。于是，对于所有 n- 类型以及具有普通边缘分布的 $P_{\tilde{L}\tilde{U}}$ 和 $P_{\bar{Y}}=P_{\tilde{Y}}$，所有 $i,\gamma>0$ 以及足够大的 n，

$$
Pr\left\{\frac{1}{\lfloor 2^{n\alpha}\rfloor}\sum_{i=1}^{\lfloor 2^{n\alpha}\rfloor} T^n_{\tilde{Y}|\tilde{L}\tilde{U}}(l^n U_i(l^n)) \cap \left[\bigcup_{j\neq 1} T^n_{\bar{Y}|\tilde{L}\tilde{U}}(l^n U_j(l^n))\right] \middle| \geqslant t_{\bar{Y}|\tilde{L}\tilde{U}} 2^{-\frac{n}{2}\gamma}\right\} < 2^{-\frac{n}{2}\gamma}
\tag{3-52}
$$

如果 $\lfloor 2^{n\alpha} \rfloor \leqslant \dfrac{t_{\tilde{U}|\tilde{L}}}{t_{\tilde{U}|\tilde{L}\tilde{Y}}} 2^{-n\gamma}$。

这里，$t_{\bar{Y}|\tilde{L}\tilde{U}}$、$t_{\tilde{U}|\tilde{Y}}$、$t_{\tilde{U}|\tilde{L}\tilde{Y}}$ 分别是 $T^n_{\bar{Y}|\tilde{L}\tilde{U}}(l^n u^n) \mid (l^n,u^n) \in T^n_{\tilde{L}\tilde{U}}$、$T^n_{\tilde{U}|\tilde{L}}(l^n) \mid l^n \in T^n_{\tilde{L}}$ 和 $T^n_{\tilde{U}|\tilde{L}\tilde{Y}}(l^n y^n) \mid (l^n,y^n) \in T^n_{\tilde{L}\tilde{Y}}$ 的通常的值。

证明：对于 $i=1,2,\cdots,\lfloor 2^{n\alpha} \rfloor$，$y^n \in T^n_{\bar{Y}} = T^n_{\tilde{Y}}$，令

$$
\hat{Z}_i(y^n) = \begin{cases} 1 & y^n \in \bigcup_{j\neq 1} T_{\bar{Y}|\tilde{L}\tilde{U}}(l^n U_j(l^n)) \\ 0 & y^n \notin \bigcup_{j\neq 1} T_{\bar{Y}|\tilde{L}\tilde{U}}(l^n U_j(l^n)) \end{cases}
\tag{3-53}
$$

及对于所有 $u^n \in T^n_{\tilde{U}|\tilde{L}}(l^n)$

$$S_i(u^n) = \left| T^n_{\tilde{Y}|\tilde{L}\tilde{U}}(l^n u^n) \cap \left[\bigcup_{j\neq i} T^n_{\tilde{Y}|\tilde{L}\tilde{U}}(l^n U_j(l^n)) \right] \right| \quad (3\text{-}54)$$

因此

$$S_i(u^n) = \sum_{y^n \in T_{\tilde{Y}|\tilde{L}\tilde{U}}(l^n u^n)} \hat{Z}_j(y^n) \quad (3\text{-}55)$$

并且

$$E\,\hat{Z}_i(y^n) = Pr\left\{ y^n \in \bigcup_{j\neq i} T^n_{\tilde{Y}|\tilde{L}\tilde{U}}(l^n U_j(l^n)) \right\} \leqslant \sum_{j\neq i} Pr\{ y^n \in T^n_{\tilde{Y}|\tilde{L}\tilde{U}}(l^n U_j(l^n)) \}$$

$$= \sum_{j\neq i} Pr\{ U_j(l^n) \in T^n_{\tilde{U}|\tilde{L}\tilde{Y}}(l^n y^n) \} = (2^{\lfloor n\alpha \rfloor} - 1)\frac{t_{\tilde{U}|\tilde{L}\tilde{Y}}}{t_{\tilde{U}|\tilde{L}}} < 2^{-n\gamma} \quad (3\text{-}56)$$

如果 $\lfloor 2^{n\alpha} \rfloor \leqslant \frac{t_{\tilde{U}|\tilde{L}}}{t_{\tilde{U}|\tilde{L}\tilde{Y}}} 2^{-n\gamma}$。

由式(3-50)和式(3-51)可得 $E\ S_i(u^n) \leqslant t_{\tilde{Y}|\tilde{L}\tilde{U}} 2^{-n\gamma}$，即，

$E[S_i(U_i(l^n)) \mid U_i(l^n)] < t_{\tilde{Y}|\tilde{L}\tilde{U}} 2^{-n\gamma}$ (类同)。于是，

$$E\ S_i(U_i(l^n)) = E\{E[S_i(U_i(l^n)) \mid U_i(l^n)]\} < t_{\tilde{Y}|\tilde{L}\tilde{U}} 2^{-n\gamma} \quad (3\text{-}57)$$

从而，根据 Markov's 不等式，有

$$Pr\left\{ \frac{1}{2^{\lfloor n\alpha \rfloor}} \sum_{i=1}^{2^{\lfloor n\alpha \rfloor}} S_i(U_i(l^n)) \geqslant t_{\tilde{Y}|\tilde{L}\tilde{U}} 2^{-\frac{n}{2}\gamma} \right\} < 2^{-\frac{n}{2}\gamma}$$

即式(3-52)。

引理 3.3　多位填充(Multi-Packing)

在前面引理的条件下，令 $U_{i,k}(l^n), i = 1,2,\cdots,\lfloor 2^{n\beta_1} \rfloor, k = 1,2,\cdots,\lfloor 2^{n\beta_2} \rfloor$ 为一给定的 $l^n \in T^n_{\tilde{L}}$ 下的独立均匀分布于 $T^n_{\tilde{U}|\tilde{L}}(l^n)$ 的序列，因此，对于所有前面引理中的 n- 类型的 $P_{\tilde{L}\tilde{U}\tilde{Y}}$ 和 $P_{\tilde{L}\tilde{U}\tilde{Y}}$

$$Pr\left\{ \frac{1}{\lfloor 2^{n\beta_2} \rfloor} \sum_{k=1}^{\lfloor 2^{n\beta_2} \rfloor} \frac{1}{\lfloor 2^{n\beta_1} \rfloor} \sum_{i=1}^{2^{n\beta_1}} \left| T^n_{\tilde{Y}|\tilde{L}\tilde{U}}(l^n U_{i,k}(l^n)) \cap \left[\bigcup_{j\neq i} T^n_{\tilde{Y}|\tilde{L}\tilde{U}}(l^n U_{i,k}(l^n)) \right] \right| \geqslant t_{\tilde{Y}|\tilde{L}\tilde{U}} 2^{-n\eta} \right\}$$
$$< 2^{-\frac{n}{2}\gamma} \quad (3\text{-}58)$$

如果

$$\lfloor 2^{n\alpha} \rfloor \leqslant \frac{t_{\tilde{U}|\tilde{L}}}{t_{\tilde{U}|\tilde{L}\tilde{Y}}} 2^{-n\gamma}$$

证明：对于 $u^n \in T^n_{\tilde{U}|\tilde{L}}(l^n)$，令

$$S_{i,k}(u^n) = \left| T^n_{\tilde{Y}|\tilde{L}\tilde{U}}(l^n u^n) \cap \left[\bigcup_{j\neq i} T^n_{\tilde{Y}|\tilde{L}\tilde{U}}(l^n U_{j,k}(l^n)) \right] \right|$$

可得到在前面式(3-57)证明中已经看到的

$$E\ S_{i,k}(U_i(l^n)) < t_{\tilde{Y}|\tilde{L}\tilde{U}} 2^{-n\gamma}$$

于是，式(3-58)可从 Markov 不等式得到。

现在，转向定理 3.12 的直接部分。

引理 3.4 (定理 3.12 的直接部分)。对于一复合信道 W

$$C_{CRI}((V,L),W,D_1) \geqslant \sup_{(V,L,U,X)\in Q_1((V,L),W,D_1)} [I(U;L,Y(W)) + H(L \mid U)] \quad (3\text{-}59)$$

证明：

我们需要证明，对于一给定的相关无记忆源具有一般的 V,L，一复合信道 W，$(V,L,$

$U,X) \in Q_1((V,L),W,D_1)$，而且足够大的 n，已存在的函数 F，G 以及 $xm(v^n,l^n)$ 满足式(3-10)～式(3-13)、式(3-22)、式(3-15)和以任意率接近 $I(U;L,Y(W))+H(L \mid U)$ 的式(3-16)。

显然，一般随机性的可达率集合是有界和封闭(紧密)的。不失一般性，根据均匀连续的信息量，可以假设 $E_\rho(V,X) < D_1$ 以及 $I(U;V,L) < I(U;L,Y(W))$。

因为 $I(U;V,L) = I(U;L)+I(U;V \mid L)$ 和 $I(U;L,Y(W)) = I(U;L)+I(U;Y(W) \mid L)$，所以存在一个足够小但正的常数 ξ，这样，

$$I(U;L(W) \mid L) - I(U;V \mid L) > \xi \tag{3-60}$$

同样，也可假设 P_U 用一 n- 类型概率简化表示。于是，对于任意 $\varepsilon_1 > 0$，根据信息量的均匀连续性，可以找到 $\delta_1,\delta_2 > 0$ 具有以下性质：

(1) 对于具有类型 $P_{l^n} = P_{\tilde{L}}$ 的所有 $l^n \in T_L^n(\delta_1)$，都存在一 $\delta' > 0$，$(v^n,l^n) \in T_{VL}^n(\delta_2')$，$T_{\tilde{V}|\tilde{L}}^n(l^n) \subset T_{V|\tilde{L}}^n(l^n,\delta_2)$。这里，$P_{\tilde{V}\tilde{L}}$ 为 (v^n,l^n) 的联合类型概率分布，且 $P_{\hat{V}\tilde{L}} = P_{\tilde{L}}P_{V|L}$。

可以把一个 $l^n \in T_L^n(\delta_1)$，$(v^n,l^n) \in T_{VL}^n(\delta_2)$，$(\delta_1,\delta_2)$ 二元组的 (v^n,l^n) 序列记为 (δ_1,δ_2)- 类型的序列 $T^n(\delta_1,\delta_2)$。

可以要求当 $\delta_1 \to 0$ 时，$\delta_2 \to 0$。更进一步(参看文献[9])，存在正数 $\zeta_1 = \zeta_1(\delta_1)$，$\zeta_2 = \zeta_2(\delta_1,\delta_2)$，$\zeta = \zeta(\delta_1,\delta_2)$，于是

$$P_L^n(T_L^n(\delta_1)) > 1 - 2^{-n\zeta_1} \tag{3-61}$$

$$P_{V|L}^n\{v^n: (v^n,l^n) \in T^n(\delta_1,\delta_2) \mid l^n) > 1 - 2^{-n\zeta_2} \tag{3-62}$$

对于 $l^n \in T_L^n(\delta_1)$，以及

$$P_{VL}^n(T^n(\delta_1,\delta_2)) > 1 - 2^{n\zeta} \tag{3-63}$$

(2) 对于所有具有类型 $P_{l^n} \in P_{\tilde{L}}$ 的 $l^n \in T_L^n(\delta_1)$，可以在 $L^n \times U^n$ 找到一个联合类型的具有边缘分布 $P_{\tilde{L}}$ 和 P_U 的序列 $P_{\tilde{L}\tilde{U}}$，，该序列足以接近 P_{LU}(将在以后特别说明)，$P_{\tilde{L}\tilde{U}}$ 由 l^n 的 $P_{\tilde{L}}$ 产生。

(3) 对于所有具有类型 $P_{v^nl^n} \in P_{\tilde{V}\tilde{L}}$ 的 $(v^n,l^n) \in T^n(\delta_1,\delta_2)$，可以找到一个在 $V^n \times L^n \times U^n$ 中的联合类型的具有边缘分布 $P_{\tilde{V}\tilde{L}}$ 和 $P_{\tilde{L}\tilde{U}}$ 而且足够接近 P_{VLU}(将在以下特别说明)的序列 $P_{\tilde{V}\tilde{L}\tilde{U}}$。这里，$P_{\tilde{L}\tilde{U}}$ 由 $P_{\tilde{L}}$ 产生。$P_{\tilde{V}\tilde{L}\tilde{U}}$ 由联合概率 $P_{\tilde{V}\tilde{L}}$ 和 (v^n,l^n) 产生。

(4) 对于所有具有联合类型 $P_{\tilde{V}\tilde{L}}$ 以及 $P_{\tilde{V}\tilde{L}}$ 产生的联合类型 $P_{\tilde{V}\tilde{L}\tilde{U}}$ 的 (δ_1,δ_2)- 序列 (v^n,l^n)，令 $(\widetilde{V},\widetilde{L},\widetilde{U},\widetilde{X})$ 为具有联合分布 $P_{\tilde{V}\tilde{L}\tilde{U}\tilde{X}}$ 的随机变量，则对于 $v \in V$，$l \in L$，$u \in U$，$x \in X$

$$P_{\tilde{V}\tilde{L}\tilde{U}\tilde{X}}(v,l,u,x) = P_{\tilde{V}\tilde{L}\tilde{U}}(v,l,u)P_{X|VLU}(x \mid v,l,u) \tag{3-64}$$

并且令 $(\widetilde{V},\widetilde{L},\widetilde{U},\widetilde{X},\widetilde{Y},(W))$ 为具有 $P_{\tilde{V}\tilde{L}\tilde{U}\tilde{X}\tilde{Y}(W)}$ 分布的随机变量，则对于 $v \in V$，$l \in L$，$u \in U$，$x \in X$，$y \in Y$

$$P_{\tilde{V}\tilde{L}\tilde{U}\tilde{X}\tilde{Y}}(v,l,u,x,y) = P_{\tilde{V}\tilde{L}\tilde{U}\tilde{X}}(v,l,u,x)W(x \mid y) \tag{3-65}$$

在式(3-64)中，任意的 $W \in w$ 以及 $P_{\tilde{V}\tilde{L}\tilde{U}\tilde{X}}$，以下不等式均成立。

$$E_\rho(\widetilde{V},\widetilde{X}) < D_1 \tag{3-66}$$

$$|H(\widetilde{L})-H(L)|<\varepsilon_1 \tag{3-67}$$

$$|I(\widetilde{U};\widetilde{V}\mid\widetilde{L})-I(U;V\mid L)|<\varepsilon_1 \tag{3-68}$$

并且

$$|I(\widetilde{U};\widetilde{Y}(w)\mid\widetilde{L})-I(U;Y(w)\mid L)|<\varepsilon_1 \tag{3-69}$$

这里，$I(\widetilde{U};\widetilde{Y}(w)\mid\widetilde{L})=\inf_{W\in w}I(\widetilde{U};\widetilde{Y}(W)\mid\widetilde{L})$。

对于任意小且固定的 ε_2，$0<\varepsilon_2<\frac{1}{2}\xi$，式(3-60)中的 ξ、ε_1 的选择太小，以至于 $\varepsilon_1<\frac{1}{2}\varepsilon_2$ 以及 $\varepsilon_1<\alpha$。

$$I(U;Y(w)\mid L)-\frac{\xi}{2}<\alpha<I(U;Y(w)\mid L)-\varepsilon_2 \tag{3-70}$$

并且，$M=2^{n\alpha}$ 是一整数。注意，根据式(3-70)，可以选择 α 任意接近 $I(U;Y(w)\mid L)-\varepsilon_2$，从而通过选择任意小的 ε_2 让其接近 $I(U;Y(w)\mid L)$。于是，通过式(3-60)、式(3-68)和式(3-70) 可得

$$\alpha>I(U;V\mid L)+\frac{\xi}{2}>I(\widetilde{U};\widetilde{V}\mid\widetilde{L})+\frac{\xi}{2}-\varepsilon_1>I(\widetilde{U};\widetilde{V}\mid\widetilde{L})+\frac{\xi}{4} \tag{3-71}$$

通过选择 $\varepsilon_1<\frac{1}{2}\varepsilon_2<\frac{1}{4}\xi$，最后的不等式成立，根据式(3-69) 和式(3-70)，有

$$\alpha<I(\widetilde{U};\widetilde{Y}(w)\mid\widetilde{L})+\varepsilon_1-\varepsilon_2<I(\widetilde{U};\widetilde{Y}(w)\mid\widetilde{L})-\frac{\varepsilon_2}{2} \tag{3-72}$$

$|T^n_{\widetilde{U}|\widetilde{L}}(l^n)|$ $l^n\in T^n_{\widetilde{L}}$ 和 $|T^n_{\widetilde{U}|\widetilde{L}}(v^n,l^n)|$ $(v^n,l^n)\in T^n_{\widetilde{V}\widetilde{L}}$ 的值分别用 $t_{\widetilde{U}|\widetilde{L}}$ 和 $t_{\widetilde{U}|\widetilde{V}\widetilde{L}}$ 表示。因此，$\frac{1}{n}\log\frac{t_{\widetilde{U}|\widetilde{L}}}{t_{\widetilde{U}|\widetilde{V}\widetilde{L}}}$ 任意接近 $I(\widetilde{U};\widetilde{V}\mid\widetilde{L})$。

这意味着，在我们的假设下，$\frac{1}{2}\varepsilon_2<\frac{1}{4}\xi$，式(3-71) 意味着，对于所有由 $(\varepsilon_1,\varepsilon_2)$ 典型序列 $P_{\widetilde{V}\widetilde{L}}$ 联合产生的类型 $P_{\widetilde{V}\widetilde{L}\widetilde{U}}$，都有

$$2^{\frac{n}{3}\varepsilon_2}\frac{t_{\widetilde{U}|\widetilde{L}}}{t_{\widetilde{U}|\widetilde{V}\widetilde{L}}}<2^{n\alpha}=M \tag{3-73}$$

下面令 $Q_w(l^nu^n,T)$ 为条件类型 $P_{\widetilde{Y}|\widetilde{L}\widetilde{U}}$ 的集合，二元组的序列 (l^n,u^n) 存在一具有 $T^n_{\widetilde{Y}|\widetilde{L}\widetilde{U}}(l^nu^n)\subset T^n_{\widetilde{Y}(W)|\widetilde{L}\widetilde{U}}(l^nu^n,T)$ 的 $W\in w$，这里，$P_{\widetilde{L}\widetilde{U}}$ 是 (l^n,u^n) 和 $P_{\widetilde{L}\widetilde{U}\widetilde{Y}(w)}$ 的类型，是式(3-65)中的边缘分布。于是

$$\bigcup_{P_{\widetilde{Y}|\widetilde{L}\widetilde{U}}\in Q_W(l^nu^n,T)}T^n_{\widetilde{Y}|\widetilde{L}\widetilde{U}}(l^nu^n,T)=\bigcup_{W\in w}T^n_{\widetilde{Y}(w)|\widetilde{L}\widetilde{U}}(l^nu^n,T) \tag{3-74}$$

并且

$$|Q_W(l^nu^n,T)|<(n+1)^{|L|u|y|} \tag{3-75}$$

再次，对于 $|T^n_{\widetilde{U}|\widetilde{L}}(l^n)|$，$l^n\in T^n_{\widetilde{L}}$ 的通常的值 $t_{\widetilde{U}\widetilde{L}}$；$T^n_{\widetilde{U}|\widetilde{L}\widetilde{Y}}(l^ny^n)$，$(l^ny^n)\in T^n_{\widetilde{L}\widetilde{Y}}$ 的通常的值 $T^n_{\widetilde{U}\widetilde{L}\widetilde{Y}}$，$\lim_{n\to\infty}\frac{1}{n}\log\frac{t_{\widetilde{U}|\widetilde{L}}}{t_{\widetilde{U}|\widetilde{L}\widetilde{Y}}}=I(\widetilde{U};\overline{Y}\mid\widetilde{L})$。

于是，式(3-72)中的结果导致所有由联合 $(l^n, u^n) \in T^n_{\tilde{L}\tilde{U}}$ 以及 $P_{\overline{Y}|\tilde{L}\tilde{U}} \in Qw(l_n u_n, T)$ 产生的 (δ_1, δ_2)-类型序列 $P_{\overline{V}\tilde{L}\tilde{U}}$，

$$M = 2^{n\alpha} < 2^{-\frac{n}{4}\varepsilon^2} \frac{t_{\tilde{U}|\tilde{L}}}{t_{\tilde{U}|\tilde{L}\overline{Y}}} \tag{3-76}$$

如果 T 很小(依赖于 ε_2)，那么对于所有 $P_{\overline{Y}|\tilde{L}\tilde{U}} \in Qw(l^n u^n, T)$

$$I(\tilde{U}; \overline{Y} \mid \tilde{L}) > I(\tilde{U}; Y(w) \mid \tilde{L}) - \frac{1}{8}\varepsilon_2$$

(回顾其定义) $I(\tilde{U}; \tilde{Y}(w) \mid \tilde{L}) > \inf\limits_{W \in w} I(\tilde{U}; \tilde{Y}(w) \mid \tilde{L})$。

3.6 编码方案

3.6.1 选择码本

对于所有具有类型 $P_{\tilde{L}}$ 由 $P_{\tilde{L}}$ 产生(参见 3.5 节)的 $P_{\tilde{L}\tilde{U}}$ 的 $l^n \in T^n_{\tilde{L}}(\delta_1)$，应用引理 3.1 取 $\eta = \frac{\varepsilon_2}{3}$ 以及引理 3.2 取 $\gamma = \frac{\varepsilon_2}{4}$ 进行随机抽取。因为 v^n、l^n 的数以及 n-联合类型分别以指数型或多项式增长，如果 n 足够大，那么对所有由 $P_{\tilde{L}}$ 产生的具有类型 $P_{\tilde{L}\tilde{U}}$ 的 $l^n \in T^n_{\tilde{L}}(\delta_1)$，通过式(3-73)和式(3-76)可以找到一个子集 $u(l^n) \in T^n_{\tilde{U}|\tilde{L}}(l^n)$，该子集具有以下特性：

如果 $(v^n, l^n) \in T^n(\delta_1, \delta_2)$ 并且具有由 $P_{\tilde{V}\tilde{L}}$ 产生的联合类型的 $P_{\tilde{V}\tilde{L}}$ 和 $P_{\tilde{V}\tilde{L}\tilde{U}}$ (参见 3.5 节)，则

$$\left| \left| u_{\tilde{U}|\tilde{V}\tilde{L}}(v^n l^n) \right| - M \frac{t_{\tilde{U}|\tilde{V}\tilde{L}}}{t_{\tilde{U}|\tilde{L}}} \right| < M \frac{t_{\tilde{U}|\tilde{V}\tilde{L}}}{t_{\tilde{U}|\tilde{L}}} \varepsilon \tag{3-77}$$

对于任意 $\varepsilon > 0$ (当 $n \to \infty, \varepsilon \to 0$)，这里，

$$u_{\tilde{U}|\tilde{V}\tilde{L}}(v^n l^n) \triangleq u(l^n) \cap T^n_{\tilde{U}|\tilde{V}\tilde{L}}(v^n l^n) \tag{3-78}$$

$P_{\tilde{V}\tilde{L}\tilde{U}}$ 由联合类型的 (δ_1, δ_2) 典型序列 (v^n, l^n) 所产生，而联合概率 $P_{\tilde{V}\tilde{L}\tilde{U}}$ 由具有边缘性质的 $P_{\tilde{L}\tilde{U}}$ 和任意 $P_{\overline{Y}|\tilde{L}\tilde{U}} \in Qw(l^n u^n_{m'}(l^n), T)$ 所产生(注意，$Qw(l^n u^n, T)$ 仅依赖于 $(l^n u^n)$ 的分布 $P_{l^n u^n}$!)。对于任意 $P_{\tilde{V}\tilde{L}\tilde{U}}$ 和任意 $P_{\tilde{L}\tilde{U}\overline{Y}}$，

$$M^{-1} \sum_{m=1}^{M} \left| T^n_{\overline{Y}|\tilde{L}\tilde{U}}(l^n \tilde{u}^n_m(l^n)) \cap \left[\bigcup_{m' \neq m} T^n_{\overline{Y}|\tilde{L}\tilde{U}}(l^n \tilde{u}^n_{m'}(l^n)) \right] \right| < 2^{-\frac{n}{8}\varepsilon_2} t_{\overline{Y}|\tilde{L}\tilde{U}} \tag{3-79}$$

如果表示 $u(l^n)$ 的元素为 $\tilde{u}^n_1(l^n)$，$\tilde{u}^n_2(l^n)$，…，$\tilde{u}^n_M(l^n)$。通过式(3-75)以及事实上的 (l^n, u^n)，(l'^n, u'^n) 具有相同的类型 $Qw(l^n u^n) = Qw(l'^n u'^n)$，则

$$M^{-1} \sum_{m=1}^{M} \left| T^n_{\overline{Y}|\tilde{L}\tilde{U}}(l^n \tilde{u}^n_m(l^n)) \cap \left[\bigcup_{m' \neq m} \bigcup_{P_{\overline{Y}|\tilde{L}\tilde{U}} \in Qw(l^n u^n_{m'}(l^n))} T^n_{\overline{Y}|\tilde{L}\tilde{U}}(l^n u^n_{m'}(l^n)) \right] \right| < 2^{-\frac{n}{9}\varepsilon_2} t_{\overline{Y}|\tilde{L}\tilde{U}} \tag{3-80}$$

我们称子集 $u(l^n)$ 为编码字 l^n 及 $\tilde{u}^n_m(l^n)$ $m = 1, 2, \cdots, M$ 的编码本(codebook)。

3.6.2 选择输入序列通过信道发送

发送者根据观察到的相关源的输出 (v^n, l^n) 以及他本人的私有随机数选择一输入序列 $x^n \in X^n$，具体如下。

在信号源的输出是具有联合类型的 $P_{\widetilde{V}\widetilde{L}}$ 的 (δ_1, δ_2) 类型序列 (v^n, l^n) 的情况下，发送者在 $U_{\widetilde{U}|\widetilde{V}\widetilde{L}}(v^n, l^n)$ 中随机均匀地选取一个序列(参见式(3-78))(如使用他自己的随机数)。也就是说，

$$\widetilde{u}_{\widetilde{m}}(l^n) U_{\widetilde{U}|\widetilde{V}\widetilde{L}}(v^n, l^n) \subset U(l^n) \tag{3-81}$$

接着，发送者选择一个具有概率 $x^n \in X^n$ 的输入序列。

$$P_{X|VLU}(x^n \mid v^n, l^n, \widetilde{u}_m^n(l^n)) \tag{3-82}$$

使用抽取的 $\widetilde{u}_m^n(l^n)$ 以及他自己的随机数，并且把它通过信道发送出去。

其他情况，例如，非 (δ_1, δ_2) 类型序列输出的情况，发送者选择一任意固定的序列，如 x_e^n，并且把它通过信道发送出去。

这里，随机抽取的码字以及信道随机输入产生的结果分别记为 U'^n 和 X'^n，将在以下分析中用到。

1) 选择函数 F、G 的支撑域为 A

令

$$J = \lfloor 2^{n(H(L)-2\varepsilon_1)} \rfloor \tag{3-83}$$

同时，令 e 为一抽象符号(代表“发生了一个错误”)。于是，定义

$$A = \{\{1,2,\cdots,M\} \times \{1,2,\cdots,J\}\} \cup \{e\} \tag{3-84}$$

2) 定义函数 F、G

为了定义函数，首先将每一 $T_{\widetilde{L}}^n \subset T_L^n(\delta_1)$ 划分为 J 个大小近似相等的子集，即每一子集的大小为 $\left\lfloor \frac{|T_{\widetilde{L}}^n|}{J} \right\rfloor$ 或者 $\left\lceil \frac{|T_{\widetilde{L}}^n|}{J} \right\rceil$，然后将集合中的第 j 个子集并集放在所有 $T_{\widetilde{L}}^n \subset T_L^n(\delta_1)$ 上，并且获得一个 $T_L^n(\delta_1)$ 的子集 L_j，以至于对于 $j = 1,2,\cdots,J$

$$|L_j \cap T_{\widetilde{L}}^n| = \left\lfloor \frac{|T_{\widetilde{L}}^n|}{J} \right\rfloor \quad 或 \quad \left\lceil \frac{|T_{\widetilde{L}}^n|}{J} \right\rceil \tag{3-85}$$

(1) 定义函数 F。

发送者观察信号源的输出而且判断函数 F 的值。

在信号源输出一个 (δ_1, δ_2) 类型序列 (v^n, l^n) 的情况下，如果 $l^n \in L_j$，根据式(3-81)中被抽取的发送者的私有随机数，F 在 (m, J) 中取值。

其他情况，$F = e$。

(2) 定义函数 G。

接收者观察相关源以及 y^n 信道输出的 L^n 的分量 l^n (边信息)判断函数 G 的值，

$$y_m(l_n) = \bigcup_{P_{\widetilde{Y}|\widetilde{L}\widetilde{U}} \in Qw(l^n \widetilde{u}_m^n(l^n), T)} T_{\widetilde{Y}|\widetilde{L}\widetilde{U}}^n(l^n \widetilde{u}_m^n(l_n), T)。$$

在 $l^n \in T_L^n(\delta_1)$ 以及存在一 $m \in \{1,2,\cdots,M\}$ 的条件下，$y^n \in y_m(l^n) \backslash \left\{ \bigcup_{m' \neq m} Y^m(l^n) \right\}$。如

果 $l^n \in L_j$，则 G 在(m, j) 中取值。注意，m 如果存在，则必须唯一。

其他情况，$G = e$。

分析：

1）失真判决

首先，再次回顾水印失真测度 ρ 的界，即

$$0 \leqslant \rho \leqslant \Delta \tag{3-86}$$

于是，根据式(3-63)，有

$$\frac{1}{n}Pr((V^n,L^n) \notin T^n_{VL}(\delta_2))E[\rho(V'^n,X'^n) \mid (V^n,L^n \notin T^n_{VL}(\delta_2)] < 2^{-n\xi}\Delta \tag{3-87}$$

另一方面，在 $(V^n,L^n) \in T^n_{\widetilde{V}\widetilde{L}} \subset T^n_{VL}(\delta_2)$ 的假设条件下，通过定义 $(V^n,L^n,U'^n) \in T^n_{\widetilde{V}\widetilde{L}\widetilde{U}}$ 具有由 $P_{\widetilde{V}\widetilde{L}}$ 产生的联合概率 $P_{\widetilde{V}\widetilde{L}\widetilde{U}}$。由式(3-65)、式(3-66)以及 (U'^n,X'^n) 的定义，有

$$\begin{aligned}
&\frac{1}{n}E[\rho(V'^n,X'^n) \mid (V^n,L^n) \notin T^n_{\widetilde{V}\widetilde{L}}] \\
&= \sum_{(v,l,u)\in V\times L\times U} P_{\widetilde{V}\widetilde{L}\widetilde{U}}(v,l,u)\sum_x P_{X|VLU}(x \mid v,l,u)\rho(v,x) \\
&= E\rho(\widetilde{V},\widetilde{X}) < D_1
\end{aligned} \tag{3-88}$$

因此，从式(3-87)和式(3-88)可得，对于足够大的 n，

$$\begin{aligned}
&\frac{1}{n}E\rho(V^n,X'^n) \\
&= Pr((V^n,L^n) \notin T^n_{VL}(\delta_2))E[\rho(V^n,X'^n) \mid (V^n,L^n) \notin T^n_{VL}(\delta_2)] \\
&\quad + \sum_{T^n_{\widetilde{V}\widetilde{L}} \subset T^n_{VL}(\delta_2)} Pr((V^n,L^n) \in T^n_{\widetilde{V}\widetilde{L}}(\delta_2))E[\rho(V^n,X'^n) \mid (V^n,L^n) \in T^n_{\widetilde{V}\widetilde{L}}] \\
&< D_1
\end{aligned} \tag{3-89}$$

2）近似均匀性的条件

由函数 F 的定义可知，$Pr\{F = e\} \leqslant Pr\{(V^n,L^n) \notin T^n_{VL}(\delta_2)\} = 1 - P^n_{VL}(T^n_{VL}(\delta_2))$，以及式(3-63)，

$$\left| Pr\{F = e\} - |A|^{-1} \right| \leqslant \max\{2^{-n\xi}, |A|^{-1}\} \to 0 \ (n \to \infty) \tag{3-90}$$

下面固定一具有 $P_{\widetilde{L}}$ 类型的 $l^n \in T^n_L(\delta_1)$，令 $P_{\widetilde{L}\widetilde{U}}$ 是通过 $P_{\widetilde{L}}$ 产生的联合概率，以及令 $Q(\widetilde{L}\widetilde{U})$ 为具有边缘分布 $P_{\widetilde{L}\widetilde{U}}$ 的联合 $P_{\widetilde{V}\widetilde{L}\widetilde{U}}$ 概率的集合，而且由某些 (δ_1,δ_2) 序列产生，于是，$Pr\{U'^n = u^n \mid L^n = l^n\} > 0$ 只在 $u^n \in U(l^n) = \{\widetilde{u}^n_m(l^n): m = 1,2,\cdots,M\}$ 的条件下成立。

此外，由编码方案，对于具有联合类型 $P_{\widetilde{V}\widetilde{L}}$ 的 (δ_1,δ_2)-类型的序列(v^n,l^n)，$\widetilde{u}^n_m(l^n) \in U(l^n)$。

$$\begin{aligned}
&Pr\{V^n = v^n,U'^n = u^n_m(l^n) \mid L = l^n\} \\
&= \begin{cases} P^n_{V|L}(V^n = v^n \mid l^n) \left| U_{\widetilde{U}|\widetilde{V}\widetilde{L}}(v^n l^n) \right|^{-1} & u^n_m(l^n) \in U_{\widetilde{U}|\widetilde{V}\widetilde{L}}(v^n l^n) \\ 0 & u^n_m(l^n) \notin U_{\widetilde{U}|\widetilde{V}\widetilde{L}}(v^n l^n) \end{cases}
\end{aligned} \tag{3-91}$$

回顾式(3-78)可知,对于所有 $l^n \in T_{\tilde{L}}^n \subset T_{\tilde{L}}^n(\delta_1)$,$\tilde{u}_m^n(l^n) \in U(l^n)$

$$\begin{aligned}&Pr\{U'^n = \tilde{u}_m^n(l^n)|L = l^n\}\\&= \sum_{P_{\tilde{V}\tilde{L}\tilde{U}} \in Q(\tilde{L}\tilde{U})} \sum_{v^n \in T^n_{\tilde{V}|\tilde{L}\tilde{U}}(l^n\tilde{u}_m^n(l^n))} P^n_{V|L}(v^n|l^n)|U_{\tilde{U}|\tilde{V}\tilde{L}}(v^n l^n)|^{-1}\end{aligned} \tag{3-92}$$

由式(3-77)可得

$$\begin{aligned}&[M(1+\varepsilon)]^{-1}\frac{|T^n_{\tilde{U}|\tilde{L}}(l^n)|}{|T^n_{\tilde{U}|\tilde{V}\tilde{L}}(v^n l^n)|} < U_{\tilde{U}|\tilde{V}\tilde{L}}(v^n l^n)|^{-1}\\&\qquad< [M(1-\varepsilon)]^{-1}\frac{|T^n_{\tilde{U}|\tilde{L}}(l^n)|}{|T^n_{\tilde{U}|\tilde{V}\tilde{L}}(v^n l^n)|}\end{aligned} \tag{3-93}$$

另一方面,

$$\begin{aligned}&\sum_{P_{\tilde{V}\tilde{L}\tilde{U}} \in Q(\tilde{L}\tilde{U})} \sum_{v^n \in T^n_{\tilde{V}|\tilde{L}\tilde{U}}(l^n\tilde{u}_m^n(l^n))} P^n_{V|L}(v^n \mid l^n)\frac{|T^n_{\tilde{U}|\tilde{L}}(l^n)|}{|T^n_{\tilde{U}|\tilde{V}\tilde{L}}(v^n l^n)|}\\&= \sum_{P_{\tilde{V}\tilde{L}\tilde{U}} \in Q(\tilde{L}\tilde{U})} \sum_{v^n \in T^n_{\tilde{V}|\tilde{L}\tilde{U}}(l^n\tilde{u}_m^n(l^n))} P^n_{V^n|L}(T^n_{\tilde{V}|\tilde{L}}(l^n) \mid l^n)\frac{|T^n_{\tilde{U}|\tilde{L}}(l^n)|}{|T^n_{\tilde{V}|\tilde{L}}(l^n)||T^n_{\tilde{U}|\tilde{V}\tilde{L}}(v^n,l^n)|}\\&= \sum_{P_{\tilde{V}\tilde{L}\tilde{U}} \in Q(\tilde{L}\tilde{U})} P^n_{V|L}(T^n_{\tilde{V}|\tilde{L}}(l^n) \mid l^n)\\&= Pr\{(V^n,l^n) \in T^n(\delta_1,\delta_2) \mid l^n\}\end{aligned} \tag{3-94}$$

这里,第一个等式成立是因为 $P^n_{V|L}(v^n \mid l^n)$ 的值为对于给定的 l^n 依赖于 v^n 的条件概率分布;第二个等式成立是基于 $\frac{t_{\tilde{U}|\tilde{L}}}{t_{\tilde{V}|\tilde{L}}t_{\tilde{U}|\tilde{V}\tilde{L}}} = \frac{t_{\tilde{U}|\tilde{L}}}{t_{\tilde{V}\tilde{U}|\tilde{L}}} = \frac{1}{t_{\tilde{V}|\tilde{L}\tilde{U}}}$ 的事实;最后一个等式成立是因为 $P_{\tilde{V}\tilde{L}\tilde{U}}$ 由 $P_{\tilde{V}\tilde{L}}$ 唯一地产生(参见 3.5 节)。

因此,结合式(3-63)、式(3-92)~式(3-94)可知:对于一 $\eta > 0$,当 $n \to \infty, \varepsilon \to 0$ 时,$\eta \to 0$。对于 $l^n \in T^n_{L(\delta_1)}$,$\tilde{u}_m^n(l^n) \in U(l^n)$,则如下:

$$(1-\eta)M^{-1} < Pr\{U'^n = \tilde{u}_m^n(l^n) \mid L = l^n\} < (1+\eta)M^{-1}, \tag{3-95}$$

于是,对于 $m \in \{1,2,\cdots,M\}, j \in \{1,2,\cdots,J\}$,

$$\begin{aligned}Pr\{F = (m,j)\} &= Pr\{U'^n = \tilde{u}_m^n(L^n), L^n \in L_j\}\\&= \sum_{l^n \in L_j} P_L^n(l^n)Pr\{U'^n = \tilde{u}_m^n(l^n) \mid L = l^n\}(1+\eta)M^{-1}P_L^n(L_j)\end{aligned} \tag{3-96}$$

因为 $|T^n_{\tilde{L}}| > 2^{n(H(\tilde{L})+\frac{\varepsilon_1}{2})}$ 对于足够大的 n,由式(3-62)和式(3-78)可知 $\frac{|T^n_{\tilde{L}}|}{J} > 2^{\frac{n}{2}\varepsilon_1}$,并且由式(3-85)可知

$$|L_j \cap T^n_{\tilde{L}}| \leqslant \left\lceil \frac{T^n_{\tilde{L}}}{J} \right\rceil < \frac{T^n_{\tilde{L}}}{J} + 1 < \frac{|T^n_{\tilde{L}}|}{J}(1 + 2^{-\frac{n}{2}\varepsilon_1})$$

因为 $P_L^n(l^n)$ 的值依赖于 l^n,这意味着,

$$P_L^n(L_j \cap T^n_{\tilde{L}}) < J^{-1}P_L^n(T^n_{\tilde{L}})(1 + 2^{-\frac{n}{2}\varepsilon})$$

从而

$$P_L^n(L_k) < P_L^n(T_L^n(\delta_1))J^{-1}(1+2^{-\frac{n}{2}\varepsilon_1}) \tag{3-97}$$

与式(3-96)结合，则

$$Pr\{F=(m,j)\} < M^{-1}J^{-1}(1+\eta)(1+2^{-\frac{n}{2}\varepsilon_1})P_L^n(T_L^n(\delta_1)) \tag{3-98}$$

类似地，可得

$$Pr\{F=(m,j)\} > M^{-1}J^{-1}(1-\eta)(1-2^{-\frac{n}{2}\varepsilon_1})P_L^n(T_L^n(\delta_1)) \tag{3-99}$$

至此，结合式(3-61)，式(3-98)和式(3-99)意味着：当 $n\to\infty,\eta\to 0$，对于一 $\eta'>0$，$\eta'\to 0$，

$$\sum_{(m,j)} |\, Pr\{F=(m,j)\} - |A|^{-1}\,| < \eta' \tag{3-100}$$

连同式(3-90)，就完成了近似均匀条件下的证明。

(1) 率。

在式(3-70)中，可选择

$$\alpha > I(U;Y(w)\mid L) - \varepsilon' \text{ 对于任何 } \varepsilon' \text{ 有 } \varepsilon_2 < \varepsilon' < \frac{1}{2}\xi$$

在式(3-63)、式(3-83)、式(3-84)和式(3-100)够大的情况下，当 $n\to\infty$，$\eta'\to 0$，对于一 $\eta''>0$，$\eta''\to 0$，

$$\begin{aligned}\frac{1}{n}H(F) &> \frac{1}{n}\log|A| - \eta'' > I(U;Y(w)\mid L) - \varepsilon' + H(L) - 2\varepsilon_1 - \eta' \\ &= I(U;Y(w)\mid L) + I(U;L) + H(L\mid U) - \varepsilon' - 2\varepsilon_1 - \eta' \\ &= I(U;Y,L(w)) + H(L\mid U) - \varepsilon' - 2\varepsilon_1 - \eta'\end{aligned}$$

(2) 错误概率的估计。

仅在以下 3 种情况下错误会发生。

情况 1：

源输出一个概率小于 $2^{-n\zeta}$ 的非 (δ_1,δ_2) 类型的序列(见式(3-63))。现在假设输出的是一具有联合分布 $P_{\tilde{V}\tilde{L}}$ 的 (δ_1,δ_2) 类型序列 (v^n,l^n)，发送者首先选择一 $\tilde{u}_m^n(l^n)\in U_{\tilde{U}|\tilde{V}\tilde{L}}(v^n,l^n)$，接着根据他的私人随机数通过信道发送 x^n，信道的输出为 $y^n\in Y^n$。接着，在情况 2 和情况 3 下错误会发生：

$$\begin{aligned}&Pr\{Y'^n=y^n\mid (V^n,L^n)=(v^n,l^n),\,U'^n=\tilde{u}_m^n(l^n)\}\\ &=\sum_{x^n\in X^n} P^n_{X|VLU}(x^n\mid v^n,l^n,\tilde{u}_m^n(l^n))W^n(y^n\mid x^n)\\ &=P^n_{\tilde{Y}(w)\tilde{V}\tilde{L}\tilde{U}}(y^n\mid v^n,l^n,\tilde{u}_m(l^n))。\end{aligned}$$

情况 2：

假设 $W\in\mathbf{W}$ 信道，抽取一码字 $\tilde{u}_m(l^n)\in U_{\tilde{U}|\tilde{V}\tilde{L}}(v^nl^n)\subset U^n(l^n)$，此时信道输出的序列

$$y^n\notin Y_m(l^n)=\bigcup_{P_{\tilde{Y}|\tilde{L}\tilde{U}}\in Qw(l^n,\tilde{u}_m(l^n))} T^n_{\tilde{Y}|\tilde{L}\tilde{U}}(l^n\tilde{u}_m(l^n),T)$$

由式(3-64)和式(3-65)，信道输出一序列 $y^n\in Y^n$ 的概率是在相关源输出 $(V^n,L^n)=(v^n,l^n)\in T^n(\delta_1,\delta_2)$ 以及抽取码字 $U'^n=\tilde{u}_m^n(l^n)\in U_{\tilde{U}|\tilde{V}\tilde{L}}(v^n,l^n)$ 的条件下产生的。

$$Pr\{y^n = Y^n \mid (V^n, L^n) = (v^n, l^n), U'^n = \tilde{u}_m^n(l^n)\}$$
$$= \sum_{x^n \in X^n} P^n_{X|VLU}(x^n \mid v^n, l^n, \tilde{u}_m^n(l^n) W^n(y^n \mid x^n))$$
$$= P^n_{\tilde{Y}(w)\tilde{V}\tilde{L}\tilde{U}}(y^n | v^n, l^n, \tilde{u}_m^n(l^n)) \tag{3-101}$$

另一方面

$$T^n_{\tilde{Y}(W)|\tilde{V}\tilde{L}\tilde{U}}(v^n l^n u_m^n(l^n), T) \subset T^n_{\tilde{Y}(W)|\tilde{L}\tilde{U}}(l^n u_m^n(l^n), T) \subset Y_m$$

因此,这样的错误发生的概率会随着 n 的指数增长而消失。

情况 3:

选择一码字 $\tilde{u}_m^n(l^n)$ 以及一信道输出 $y^n \in Y_m \cap \left[\bigcup_{m' \neq m} Y_{m'}\right]$。由式(3-91)、式(3-93)和式(3-95),并且经过简单计算,可得

$$[(1-\eta)(1-\varepsilon)]^{-1} P^n_{V|L}(v^n l^n) \frac{t_{\tilde{U}|\tilde{L}}}{t_{\tilde{U}|\tilde{V}\tilde{L}}} < Pr\{V^n = v^n \mid L^n = l^n, U'^n = \tilde{u}_m^n(l^n)\}$$
$$< [(1+\eta)(1+\varepsilon)]^{-1} P^n_{V|L}(v^n \mid l^n) \frac{t_{\tilde{U}|\tilde{L}}}{t_{\tilde{U}|\tilde{V}\tilde{L}}} \tag{3-102}$$

对于具有联合概率 $P_{\tilde{V}\tilde{L}}$ 以及 $\tilde{u}_m(l^n) \in U_{\tilde{U}|\tilde{V}\tilde{L}}(v^n, l^n)$ 的 (δ_1, δ_2) 典型序列 (v^n, l^n),这里,$P_{\tilde{V}\tilde{L}\tilde{U}}$ 由 $P_{\tilde{V}\tilde{L}}$ 产生。因为 $t_{\tilde{U}|\tilde{V}\tilde{L}} = \frac{t_{\tilde{V}\tilde{U}|\tilde{L}}}{t_{\tilde{V}|\tilde{L}}}$, $t_{\tilde{U}\tilde{V}|\tilde{L}} = t_{\tilde{U}|\tilde{L}} t_{\tilde{V}|\tilde{L}\tilde{U}}$,对于给定的 l^n, $P^n_{V|L}(v^n \mid l^n)$ 的值通过条件概率依赖于 v^n。

$$P^n_{V|L}(v^n l^n) \frac{t_{\tilde{U}|\tilde{L}}}{t_{\tilde{U}|\tilde{V}\tilde{L}}} = P^n_{V|L}(v^n l^n) \frac{t_{\tilde{V}|\tilde{L}}}{t_{\tilde{V}|\tilde{L}\tilde{U}}} = P^n_{V|L}(T^n_{\tilde{V}|\tilde{L}}(l^n) \mid l^n) \frac{1}{t_{\tilde{V}|\tilde{L}\tilde{U}}} \tag{3-103}$$

$$(v^n, l^n, u^n) \in T^n_{\tilde{V}\tilde{L}\tilde{U}}, \lim_{n\to\infty} \frac{1}{n}\left(\log P^n_{\tilde{V}|\tilde{L}\tilde{U}}(v^n \mid l^n, u^n) - \log \frac{1}{t_{\tilde{V}|\tilde{L}\tilde{U}}}\right) = 0 \tag{3-104}$$

对于具有联合概率 $P_{\tilde{V}\tilde{L}}$ 类型的 (δ_1, δ_2) 典型序列 (v^n, l^n),$\tilde{u}_m(l^n) \in U_{\tilde{U}|\tilde{V}\tilde{L}}(v^n, l^n)$ 以及足够大的 n,当 $n \to \infty, \theta \to 0$,选取 $\theta < \frac{1}{20}\varepsilon_2$。

因为 $Pr\{(V^n, L^n) = (v^n, l^n), U'^n = u^n\} > 0$ 只有在 (v^n, l^n) 是 (δ_1, δ_2) 类型以及 $u^n \in U_{\tilde{U}|\tilde{V}\tilde{L}}(v^n, l^n)$ 下,由式(3-101)和式(3-104)可得

$$Pr\{Y'^n = y^n \mid L^n = l^n, U'^n = \tilde{u}_m^n(l^n)\}$$
$$= \sum_{v^n \in V^n} Pr\{V^n = v^n \mid L^n = l^n, U'^n = \tilde{u}_m(l^n)\}$$
$$Pr\{Y'^n = y^n \mid (V^n, L^n) = (v^n, l^n), U'^n = \tilde{u}_m^n(l^n)\}$$
$$\leqslant \sum_{v^n \in V^n} 2^{n\theta} P^n_{\tilde{V}|\tilde{L}\tilde{U}}(v^n \mid l^n, u_m^n(l^n)\} P^n_{\tilde{Y}(W)|\tilde{V}\tilde{L}\tilde{U}}(y^n \mid v^n, l^n, u^n)$$
$$\leqslant 2^{n\theta} P^n_{\tilde{Y}(W)|\tilde{L}\tilde{U}}(y^n \mid l^n, u_m^n(l^n)) \tag{3-105}$$

对于 $l^n \in T^n_L(\delta_1)$, $\tilde{u}_m(l^n) \in U(l^n)$ 以及 $y^n \in Y^n$,如果 $W \in \mathbf{W}$ 信道,可获得一个用乘积概率分布 $P^n_{\tilde{Y}(\tilde{w})|\tilde{L}\tilde{U}}(y^n \mid l^n, u_m^n(l^n))$ 表示的上界,其值通过条件概率依赖于 Y^n。结果由式(3-80)和式(3-105)可知:对于所有具有联合概率 $P_{\tilde{L}\tilde{U}}, P_{\tilde{Y}|\tilde{L}\tilde{U}} \in Qw(l^n \tilde{u}_m(l^n), T)$,

$l^n \in T_L^n(\delta_1)$，$\widetilde{u}_m^n(l^n) \in U(l^n)$ 以及足够大的 n，

$$M^{-1}\sum_{m=1}^{M} Pr\left\{Y'^n \in T^n_{Y|L\widetilde{U}}(l^n,u_m^n(l^n)) \cap \left[\bigcup_{m'\neq m} Y_{m'}(l^n)\right] \mid L^n = l^n, U'^n = \widetilde{u}_m^n(l^n)\right\}$$

$$< (n+1)^{|L||\widetilde{U}||Y|}2^{-\frac{n}{20}\varepsilon_2}$$

$$< 2^{-\frac{n}{21}\varepsilon_2} \tag{3-106}$$

最后，由式(3-95)和式(3-106)，我们获得了一个在条件 $L^n = l^n \in T_L^n(\delta_1)$ 下的错误类型发生概率的上限

$$\sum_{m=1}^{M} Pr\{U'^n = \widetilde{u}_m(l^n)|L^n = l^n\} Pr\left\{Y'^n \in y_m(l^n) \cap \left[\bigcup_{m'\neq m} Y_{m'}(l^n)\right] |L^n = l^n, U'^n = \widetilde{u}_m(l^n)|\right\}$$

$$< (1+\eta)\sum_{m=1}^{M} M^{-1} Pr\left\{Y'^n \in y_m(l^n) \cap \left[\bigcup_{m'\neq m} Y_{m'}(l^n)\right] |L^n = l^n, U'^n = \widetilde{u}_m(l^n) \mid\right\}$$

$$< (1+\eta)2^{-\frac{n}{21}\varepsilon_2} \tag{3-107}$$

因为定义：对于所有 $l^n \in T_L^n(\delta_1)$，$\sum_{m=1}^{M} Pr\{U'^n = \widetilde{u}_m(l^n) \mid L^n = l^n\} = 1$，因此完成了证明。

推论 3.1(定理 3.10 的直接部分)：对于所有单个信道 W

$$C_{CRI}((V,L),W,D_1) \geqslant \max_{(V,L,U,X,Y)\in Q((V,L),W,D_1)} [I(U;L,Y) + H(L \mid U)] \tag{3-108}$$

引理 3.5(定理 3.12 的直接部分)：对于所有复合信道 W

$$C_{CRII}((V,L),W,R_K,D_1) \geqslant \sup_{(V,L,U,X)\in Q_1^*((V,L),w,R_K D_1)} [I(U;L,Y(w)) + H(L \mid U)] + R_K \tag{3-109}$$

证明：和以前引理的证明一样，对于复合 $E\rho(V,X) < D_1$ 以及某些 $\xi > 0$ 的 (V,L,U,X)，已足以证明 $I(U;LY(w)) + H(L \mid U) + R_K$ 的可达性

$$I(U;Y(w) \mid L) + R_K - I(U;V \mid L) > \xi \tag{3-110}$$

在 $I(U;Y(w) \mid L) > I(U;V \mid L)$ 的情况下，由前面的引理可知：在无噪声信道缺失的情况下，$I(U;LY(w)) + H(L \mid U)$ 也是可达的。因此，发送者和接收者之间也许会产生 $n(I(U;LY(w)) + H(L \mid U))$ 比特的一般随机量。同时，发送者通过无噪声信道向接收者发送 R_K 比特的私有随机数造成 nR_K 比特的额外的随机量。这就是说，随机量的概率为 $I(U;L,Y(w)) + H(L \mid U) + R_K$ 时是可达的。

下面假设 $I(U;Y(w) \mid L) \leqslant I(U;V; \mid L)$。进一步，可假设 $I(U;Y(w) \mid L) > 0$，因为 $I(U;L,Y(w)) + H(L \mid U) + R_K = I(U;L) + H(L \mid U) + R_K = H(L) + R_K$，其可达性如下：

在证明前面引理的编码方案中，将 $T_L^n(\delta_1)$ 划分成 $L_j, j = 1,2,\cdots,J$ 获得了 $n(H(L) - 2\varepsilon_1)$ 比特的公共随机量。另外，通过无噪声信道也得到了 nR_K 比特的随机量。于是，足以假设：对于一 $0 < \xi < R_K$ 的 ξ，

$$0 < I(U;Y(w) \mid L) \leqslant I(U;V \mid L) < I(U;Y(w) \mid L) + R_K - \xi \tag{3-111}$$

我们将使用具有联合概率 $P_{\tilde{L}\tilde{U}}P_{\tilde{V}\tilde{L}\tilde{U}}$ 的 (δ_1,δ_2) 序列，以及定义在前面引理证明中满足式(3-65)～式(3-69)的式(3-64)和式(3-65)中的随机变量 $(\tilde{V},\tilde{L},\tilde{U},\tilde{X})$ 和 $(\tilde{V},\tilde{L},\tilde{U},\tilde{X},\tilde{Y}(w))$ 代替式(3-70)中的 α，现在选择 $\beta_1,\beta_2>0$ 和 $\beta_3\geqslant 0$，对于任意小但固定的 ε_2，$0<\varepsilon_2<\frac{1}{2}\xi$，这样

$$I(U;Y(w)\mid L)-\frac{3}{2}\varepsilon_2<\beta_1<I(U;Y(w)\mid L)-\varepsilon_2 \tag{3-112}$$

$$I(U;V\mid L)-I(U;Y(w)\mid L)+\xi\leqslant\beta_2\leqslant R_K \tag{3-113}$$

并且

$$0\leqslant\beta_3=R_K-\beta_2 \tag{3-114}$$

注意，式(3-114)保证了 β_2 存在而且是正的。

将不等式(3-112)和不等式(3-113)的两边相加，可得

$$\beta_1+\beta_2>I(U;V\mid L)+\left(\xi-\frac{3}{2}\varepsilon_2\right) \tag{3-115}$$

并且，由式(3-112)和式(3-114)中的第一个不等式，可得

$$\beta_1+\beta_2+\beta_3>I(U;Y(w)\mid L)+R_K-\frac{3}{2}\varepsilon_2 \tag{3-116}$$

令 $\xi-\frac{3}{2}\varepsilon_2=2\eta$ 并且重写式(3-116) 为

$$\beta_1+\beta_2>I(U;V\mid L)+2\eta \tag{3-117}$$

通过选择 $\varepsilon_2<\frac{1}{2}\xi$，可得 $\eta>\frac{\xi}{8}>0$。

下面与前面引理的证明一样，固定一任意小的正数 ε_2、η，选择足够小的 ε_1，这样 $\varepsilon_1<\min\left(\frac{1}{2}\varepsilon_2,\frac{1}{2}\eta\right)$。于是，由式(3-69)和式(3-114)中的第二个不等式，可得

$$\beta_1<I(\tilde{U};\tilde{Y}(w)\mid\tilde{L})-\frac{\varepsilon_2}{2} \tag{3-118}$$

并且，由式(3-70)和式(3-117)，有

$$\beta_1+\beta_2>I(\tilde{U};\tilde{V}\mid\tilde{L})+\frac{3}{2}\eta \tag{3-119}$$

不失一般性，假设 $2^{n\beta_1}$、$2^{n\beta_2}$ 和 $2^{n\beta_3}$ 都为整数，而且记为 $M_1=2^{n\beta_1}$，$I=2^{n\beta_2}$，$K'=2^{n\beta_3}$。

与前面引理的证明相似，我们知道，对于足够大的 n、足够小的 T，所有由 (δ_1,δ_2) 典型序列产生的联合概率 $P_{\tilde{V}\tilde{L}\tilde{U}}$ 以及在前面引理证明中的 $Qw(l^n u^n,T)$

$$2^{n\eta}\frac{t_{\tilde{U}|\tilde{L}}}{t_{\tilde{U}|\tilde{V}\tilde{L}}}<M_1 I \tag{3-120}$$

而且

$$M_1<2^{-\frac{n}{3}\varepsilon_2}\frac{t_{\tilde{U}|\tilde{L}}}{t_{\tilde{U}|\tilde{L}\tilde{Y}}} \tag{3-121}$$

对所有 $P_{\tilde{Y}|\tilde{L}\tilde{U}}\in Qw(l^n u^n,T)$ 都成立。

编码方案：

1）选择码本

对所有 $l^n \in T_L^n(\delta_1)$，分别用 $\alpha = \beta_1 + \beta_2$ 以及 $\gamma = \frac{\varepsilon_2}{3}$ 替换定理 3.18 和定理 3.19 中的 α 和 γ 的方式选择一码本。于是，通过随机抽取，获得了子集合 $T_{\tilde{U}}^n U^i(l^n) = \{\tilde{u}_{m,i}^n(l^n):m=1,2,\cdots,M_1\}$，其中 $i=1,2,\cdots,I$。如此，对于所有 $l^n \in T_L^n(\delta_1)$

$$U^*(l^n) = \bigcup_{i=1}^{I} U^i(l^n) \tag{3-122}$$

并且，$U_{\tilde{U}|\tilde{V}\tilde{L}}^*(v^n l^n) = U^*(l^n) \cap T_{\tilde{U}|\tilde{V}\tilde{L}}^n(v^n, l^n)$，$(v^n, l^n)$ 同前，并且混用式(3-122)中的符号：如果其中一个码字重复出现，就计数两次并将其标记为不同的元素 $\tilde{u}_{m,i}^n(l^n)$ 和 $\tilde{u}_{m',i'}^n(l^n)$，则式(3-123)成立。

$$\left| U_{\tilde{U}|\tilde{V}\tilde{L}}^*(v^n l^n) - M_1 I \frac{t_{\tilde{U}|\tilde{V}\tilde{L}}}{t_{\tilde{U}|\tilde{V}\tilde{L}}} \right| < M_1 I \frac{t_{\tilde{U}|\tilde{V}\tilde{L}}}{t_{\tilde{U}|\tilde{V}\tilde{L}}} \varepsilon \tag{3-123}$$

而且，对于 $Qw(l^n v^n, T)$ 以及任意条件概率 $P_{\tilde{Y}|\tilde{L}\tilde{U}}$

$$I^{-1} \sum_{i=1}^{I} M_1^{-1} \sum_{m=1}^{M_1} \left| T_{\tilde{Y}|\tilde{L}\tilde{U}}^n(l^n u_{m,i}^n(l^n)) \cap \left[\bigcup_{m' \neq m} \bigcup_{P_{\tilde{Y}|\tilde{L}\tilde{U}} \in Qw(l^n v^n)} T_{\tilde{Y}|\tilde{L}\tilde{U}}^n(l^n u_{m',i}^n(l^n)) \right] \right| \tag{3-124}$$

这里，式(3-123)和式(3-124) 分别类似于式(3-77)和式(3-80)，它们的证明也类似。

2）信道输入的选择

在目前的模型中，除了在模型Ⅰ中存在有噪信道外，另外还具有 R_K 率的无噪信道，发送者选择两个信道的输入如下。

(1) 选择有噪信道的输入序列。

在源输出一具有联合概率 $P_{\tilde{V}\tilde{L}}$ 的 (δ_1, δ_2) 典型序列 (v^n, l^n) 的情况下，由式(3-124)，对于由 $P_{\tilde{V}\tilde{L}}$ 产生的类型 $P_{\tilde{V}\tilde{L}\tilde{U}}$，$U_{\tilde{U}|\tilde{V}\tilde{L}}^*(v^n l^n) \neq \varnothing$。发送者随机且均匀选择 $U_{\tilde{U}|\tilde{V}\tilde{L}}^*(v^n l^n)$ 的一个元素，如 $\tilde{u}_{m,i}^n(l^n)$，并且根据概率 $P_{X|VLU}(x^n \mid v^n, l^n, \tilde{u}_{m,i}^n(l^n))$ 选择一个输入序列 x^n，通过信道发向接收者。

在信源输出是非 (δ_1, δ_2) 典型序列的情况下，发送者通过信道发送一任意固定的序列 x_e^n。

(2) 选择无噪声信道的输入。

在相关的信道输出为具有联合概率 $P_{\tilde{V}\tilde{L}}$ 的 (δ_1, δ_2) 序列 (v^n, l^n) 的情况下，发送者首先花费 $\log I = n\beta_2$ 比特通过无噪信道将索引号 $i \in \{1,2,\cdots,I\}$ 发送至接收者。如果码字 $\tilde{u}_{m,i}^n(l^n) \in U^i(l^n) \subset U^*(l^n)$ 在当前的编码方案步骤(1)中被抽取，那么发送者利用其余的 $nR_K - n\beta_2 = n\beta_3 = \log K'$ 比特，随机且均匀地抽取一独立于信源输出的 $k' \in \{1,2,\cdots,K'\}$ 并且把它通过无噪信道发出。

在一非 (δ_1, δ_2) 序列输出的情况下，发送者通过无噪声信道发送一恒定消息。

3）抽取函数 F 和 G 的公共域 A

令 J 和式(3-83)中的一样，且

$$A = [\{1,2,\cdots,M_1\} \times \{1,2,\cdots,I\} \times \{1,2,\cdots,K'\} \times \{1,2,\cdots,J\}] \cup \{e\} \tag{3-125}$$

4）定义函数 F 和 G

在证明前面引理的编码方案中，划分 $T_L^n(\delta_1)$ 为 $L_j, j=1,2,\cdots,J$，并且令 $K_n=\{1,2,\cdots,I\}\times\{1,2,\cdots,K'\}$。

（1）定义函数 F

发送者根据相关源的输出以及他自己的私有随机数选定函数 F 的值。

在输出一 (δ_1,δ_2) 序列 (v^n,l^n) 的情况下，如果在目前编码方案中抽取的 $l^n\in L_j$，$\tilde{u}^n_{m,i}(l^n)\in U_j(l^n)\cap U^*_{\tilde{U}|\tilde{V}\tilde{L}}(v^n l^n)$，则 F 取值 (m,i,k',j)。用抽取的 k' 将其在无噪声信道的最后 $n\beta_3$ 比特中发送（这意味着，(i,k') 已通过无噪信道发过）。

其他情况：$F=e$。

（2）定义函数 G

接收方根据无噪信道的输出 $(i,k')\in K_n$、相关源 L^n 的输出分量 l^n，以及含噪复合信道 W 的输出 $y^n\in Y^n$ 决定函数 G 的值。如下：

对于 $m=1,2,\cdots,M_1, i=1,2,\cdots,I$，令

$$Y_{m,i}(l^n)=\bigcup_{P_{\tilde{Y}|\tilde{L}\tilde{U}}\in Qw(l^n\tilde{u}^n_{m,i}(l^n),T)} T^n_{\tilde{Y}|\tilde{L}\tilde{U}}(l^n u^n_m, i(l^n))$$

如果无噪信道的输出为 (i,k')，$l^n\in T_L^n(\delta_1)$ 是源输出，且存在一 $m\in\{1,2,\cdots,M_1\}$，使得有噪复合信道 W 的输出 $y^n\in Y_{m,i}(l^n)\setminus\left\{\bigcup_{m'\neq m} y_{m',i}(l^n)\right\}$，若 $l^n\in L_j$，则 G 取值于 (m,i,k',j)。

其他情况：$G=e$。

分析：

1）失真准则、近似均匀条件以及率

可以确认失真准则、近似均匀条件以及率

$$\frac{1}{n}\log H(F)>\beta_1+\beta_2+\beta_3+o(1)=I(U;Y(w)\mid L)+R_K+o(1)$$

参考式(3-117)，获得类似的不等式

$$(1-\eta)(M_1 I)^{-1}<Pr\{U'^n=u^n_{m,i}(l^n)\mid L=l^n\}<(1+\eta)(M_1 I)^{-1} \tag{3-126}$$

2）估计错误概率

首要两种类型的错误概率是由一非 (δ_1,δ_2) 类型序列输出产生以及由 $\tilde{u}_{m,i}(l^n)$ 错误抽取所致的，而且输出的噪声符合信道的输出 $y^n\in Ym,i(l^n)$ 随着 n 的增加指数性地消失。

下面用 $U^i(l^n)$ 和式(3-125)替换 $U(l^n)$ 和式(3-80)，如同前面引理的证明，可以获得

$$(M_1 I)^{-1}\sum_{i=1}^{I}\sum_{m=1}^{M_1}Pr\left\{Y'^n\in Y_{m,i}(l^n)\cap\left[\bigcup_{m'\neq m}Y_{m',i}(l^n)\right]\middle| L^n=l^n, U'n=u^n_{m,i}(l^n)\right\} \tag{3-127}$$

代替式(3-106)，最后类似地由式(3-95)和式(3-106)获得式(3-107)，最后结合式(3-126)和式(3-127)完成证明。

3.7 对于随机性的逆定理

为了获得对于随机性编码定理单一字母特性，需要一个有用的引理证明，这个引理[5]的详细论证如下。

引理 3.6 令 (A^n,B^n) 是一任意随机序列对，并且令 C 是一任意随机变量，于是，

$$H(A^n|C)-H(B^n|C)$$
$$=\sum_{t=1}^{n}[H(A_t|A_{t+1},A_{t+2},\cdots,A_n,B^{t-1},C)-H(B_t|A_{t+1},A_{t+2},\cdots,A_n,B^{t-1},C)] \quad (3\text{-}128)$$

证明：

$$\begin{aligned}
&H(A^n|C)-(B^n|C)\\
&=\sum_{t=0}^{n-1}H(A_{t+1},A_{t+2},\cdots,A_n,B^t|C)-\sum_{t=1}^{n}H(A_{t+1},A_{t+2},\cdots,A_n,B^t|C)\\
&=\sum_{t=1}^{n}H(A_t,A_{t+1},\cdots,A_n,B^{t-1}|C)-\sum_{t=1}^{n}H(A_{t+1},A_{t+2},\cdots,A_n,B^t|C)\\
&=\sum_{t=1}^{n}[H(A_t,A_{t+1},\cdots,A_n,B^{t-1}|C)-H(A_{t+1},\cdots,A_n,B^{t-1}|C)]\\
&-\sum_{t=1}^{n}[H(A_{t+1},A_{t+2},\cdots,A_n,B^t|C)-H(A_{t+1},\cdots,A_n,B^{t-1}|C)]\\
&=\sum_{t=1}^{n}[H(A_t|A_{t+1},\cdots,A_n,B^{t-1},C)-H(B_t|A_{t+1},\cdots,A_n,B^{t-1},C)]\\
&=\sum_{t=1}^{n}[H(A_t|A_{t+1},\cdots,A_n,B^{t-1},C)-H(B_t|A_{t+1},\cdots,A_n,B^{t-1},C)] \qquad (3\text{-}129)
\end{aligned}$$

这里，当 $t=0$ 和 $t=n$ 时，$(A_{t+1},A_{t+2},\cdots,A_n,B^t)$ 可分别被理解为 A^n 和 B^n。

引理 3.7(定理 3.8 的逆部分) 对单一信道 W

$$C_{CRI}((V,L),W,D_1)\leqslant\max_{(V,L,U,X,Y)\in Q((V,L),W,D_1)}[I(U;LY)+H(L|U)] \quad (3\text{-}130)$$

证明： 假设对于一个 n 长的源输出序列，存在函数 F 和 K 使得对于信道 W^n 和式(3-10)～式(3-16)成立。记 X^n 和 Y^n 分别为有相关源 (V^n,L^n) 所产生的输入和输出，记发送者的私人随机数为 M，于是，式(3-10)中用 (V^n,L^n) 重写为

$$\frac{1}{n}E\rho(V^n,X^n)\leqslant D_1 \quad (3\text{-}131)$$

进一步，由 Fano 不等式式(3-11)～式(3-14)，有

$$\begin{aligned}
H(F)&\leqslant H(F)-H(F|G)+n\lambda\log k+h(\lambda)\\
&=I(F;G)+n\lambda\log k+h(\lambda)\\
&\leqslant I(F;L^n,Y^n)+n\lambda\log k+h(\lambda)\\
&=I(F;Y^n|L^n)+I(F;L^n)+n\lambda\log k+h(\lambda)\\
&\leqslant I(F;Y^n|L^n)+H(L^n)+n\lambda\log k+h(\lambda)
\end{aligned}$$

$$= I(F;Y^n|L^n) + \sum_{t=1}^{n} H(L_t) + n\lambda \log k + h(\lambda)$$

$$= \sum_{t=1}^{n} I(F;Y_t|L^n,Y^{t-1}) + \sum_{t=1}^{n} H(L_t) + n\lambda \log k + h(\lambda) \quad (3\text{-}132)$$

这里，对于 $z \in [0,1]$，$h(z) = -z\log z - (1-z)\log(1-z)$ 是二进制的熵。这里，第一个不等式由 Fano 不等式(3-11)、式(3-12)和式(3-14)而来，第二个不等式由式(3-13)得来；第三个不等式成立是因为源是无记忆的。因为 $I(F;V_n,L_n) \leqslant H$，紧随式(3-132)前面 4 行，

$$\begin{aligned}
0 &\leqslant I(F;L^n,Y^n) - I(F;V^n,L^n) + n\lambda \log k + h(\lambda) \\
&\leqslant [I(F;L^n|Y^n) + I(F;L^n)] - [I(F;V^n|L^n) + I(F;L^n)] + n\lambda \log k + h(\lambda) \\
&= I(F;L^n|Y^n) - I(F;V^n|L^n) + n\lambda \log k + h(\lambda) \\
&= [H(Y^n|L^n) - H(Y^n|L^n,F)] - [H(V^n|L^n) - H(V^n|L^n,F)] + n\lambda \log k + h(\lambda) \\
&= [H(Y^n|L^n) - H(V^n|L^n)] + [H(V^n|L^n,F) - H(Y^n|L^n,F)] + n\lambda \log k + h(\lambda)
\end{aligned} \quad (3\text{-}133)$$

为了获得单一字母特性，分别用 V^n、Y^n、(L^n,F) 替代式(3-129)中的 A^n、B^n、C，于是

$$H(V^n|L^n,F) - H(Y^n|L^n,F)$$

$$= \sum_{t=1}^{n} [H(V_t|V_{t+1},V_{t+2},\cdots,V_n,L^n,Y^{t-1},F) - H(Y_t|V_{t+1},V_{t+2},\cdots,V_n,L^n,Y^{t-1},F)] \quad (3\text{-}134)$$

更进一步，因为源是无记忆的，因此有

$$H(V^n|L^n) = \sum_{t=1}^{n} H(V_t|L_t) \quad (3\text{-}135)$$

将式(3-132)以及 $H(Y^n|L^n) = \sum_{t=1}^{n} H(Y_t|L^n,Y^{t-1})$ 代入式(3-133)～式(3-135)，得到

$$\begin{aligned}
0 &\leqslant \sum_{t=1}^{n} [H(Y_t|L^n,Y^{t-1}) - H(V_t|L_t)] + \sum_{t=1}^{n} [H(V_t|V_{t+1},V_{t+2},\cdots,V_n,L^n,Y^{t-1},F) \\
&\quad - H(Y_t|V_{t+1},V_{t+2},\cdots,V_n,L^n,Y^{t-1},F)] + n\lambda \log k + h(\lambda) \\
&= \sum_{t=1}^{n} [H(Y_t|L^n,Y^{t-1}) - H(Y_t|V_{t+1},V_{t+2},\cdots,V_n,L^n,Y^{t-1},F)] \\
&\quad - \sum_{t=1}^{n} [H(V_t|L_t)] - H(V_t|V_{t+1},V_{t+2},\cdots,V_n,L^n,Y^{t-1},F)] + n\lambda \log k + h(\lambda) \\
&= \sum_{t=1}^{n} I(Y_t;V_{t+1},V_{t+2},\cdots,V_n,F|L^n,Y^{t-1}) \\
&\quad - \sum_{t=1}^{n} I(V_t;V_{t+1},V_{t+2},\cdots,V_n,L_1,L_2,\cdots,L_{t-1},L_{t+1},\cdots,L_n,Y^{t-1},F|L_t) + n\lambda \log k + h(\lambda) \\
&\leqslant \sum_{t=1}^{n} [I(Y_t;V_{t+1},V_{t+2},\cdots,V_n L_1,L_2,\cdots,L_{t-1},L_{t+1},\cdots,L_n,Y^{t-1},F|L_t)]
\end{aligned}$$

$$- \sum_{t=1}^{n} I(V_t; V_{t+1}, V_{t+2}, \cdots, V_n, L_1, L_2, \cdots, L_{t-1}, L_{t+1}, \cdots, L_n, Y^{t-1}, F|L_t)]$$

$$+ n\lambda \log k + h(\lambda) \tag{3-136}$$

令 J 为在 $\{1,2\cdots,n\}$ 均匀可变取值，并且

$$U_J = (V_{J+1}, V_{J+2}, \cdots, V_n, L_1, L_2, \cdots, L_{J-1}, L_{J+1}, \cdots, L_n, Y^{J-1}, F) \tag{3-137}$$

由于 J 和 (V_J, L_J) 是独立的，即 $I(J, V_J, L_J) = 0$，于是重写式(3-131)并且继续以下几行。

$$\begin{aligned} 0 &\leqslant nI(U_J; Y_J|L_J, J) - nI(U_J; V_J|L_J, J) + n\lambda \log k + h(\lambda) \\ &= n[I(U_J; L_J, Y_J|J) - I(U_J; L_J|J)] - [I(U_J; V_J|L_J, J) \\ &\quad - I(U_J; L_J|J) + n\lambda \log k + h(\lambda) \\ &= nI(U_J; L_J, Y_J|J) - nI(U_J; V_J, L_J|J) + n\lambda \log k + h(\lambda) \\ &\leqslant nI(U_J, J; L_J, Y_J) - n[I(U_J, J; V_J, L_J) - I(J; V_J, L_J)] + n\lambda \log k + h(\lambda) \\ &= nI(U_J, J; L_J, Y_J) - nI(U_J, J; V_J, L_J) + n\lambda \log k + h(\lambda) \end{aligned} \tag{3-138}$$

下面记

$$(V'', L'', U'', X'', Y'') = (V_J, L_J U_J J, X_J, Y_J) \tag{3-139}$$

对于式(3-137)中均匀分布的 J 和 U_J，显然，由相关源 (V, L) 产生的 (V'', L'') 具有相同的概率分布，条件概率分布 $P_{Y''|X''} = W$ 以及 $(V''L''U'', X'', Y'')$ 形成一马尔可夫链。也就是说，$(V'', L'', U'', X'', Y'')$ 的联合分布为 $P_{V''L''U''X''Y''} = P_{VL} P_{U''X''|V''L'} W$。连同式(3-131)，可重写为

$$\begin{aligned} E\rho(V'', X'') &= E[E\rho(V'', X'')|J] = E[E\rho(V_J, X_J)|J] \\ &= \frac{1}{n} E\rho(V^n, X^n) \leqslant D_1 \end{aligned} \tag{3-140}$$

进一步，在式(3-138)中通过替换(*)并且在结果不等式两边同时除以 n，得到

$$0 \leqslant I(U''; L'', Y'') - I(U''; V'', L'') + o(1) \qquad \lambda \to 0 \tag{3-141}$$

因为集合 $\{P_{V,L,U,X,Y}: (V, L, U, X, Y) \in Q((V, L), W, D_1)\}$ 是紧凑的，由式(3-139)和式(3-140)足以完成证明

$$\frac{1}{n} H(F) \leqslant I(U''; L'', Y'') + H(L''|U'') + o(1)$$

对于 $\lambda \to 0$，可以通过在式(3-132)两边同时除以 n 继续进行以下几个步骤。

$$\begin{aligned} &\frac{1}{n} H(F) \\ &\leqslant \frac{1}{n} \sum_{t=1}^{n} I(F; Y_t | L^n, Y^{t-1}) + \frac{1}{n} \sum_{t=1}^{n} H(L_t) + \lambda \log k + \frac{1}{n} h(\lambda) \\ &\leqslant \frac{1}{n} \sum_{t=1}^{n} I(V_{t+1}, V_{t+2}, \cdots, V_n, F; Y_t | L^n, Y^{t-1}) + \frac{1}{n} \sum_{t=1}^{n} H(L_t) + \lambda \log k + \frac{1}{n} h(\lambda) \\ &\leqslant \frac{1}{n} \sum_{t=1}^{n} I(V_{t+1}, V_{t+2}, \cdots, V_n, L_1, L_2 \cdots, L_{t-1}, L_{t+1}, \cdots, L_n, Y^{t-1}, F; Y_t | L_t) \\ &\quad + \frac{1}{n} \sum_{t=1}^{n} H(L_t) + \lambda \log k + \frac{1}{n} h(\lambda) \end{aligned}$$

$$= I(U_J;Y_J|L_J,J)+H(L_J|J)+\lambda\log k+\frac{1}{n}h(\lambda)$$

$$\leqslant I(U_J,J;Y_J|L_J)+H(L_J|J)+\lambda\log k+\frac{1}{n}h(\lambda)$$

$$= I(U_J,J;Y_J|L_J)+H(L_J)+\lambda\log k+\frac{1}{n}h(\lambda)$$

$$= I(U_J,J;Y_J|L_J)+I(U_J;L_J)+H(L_J|U_J)+\lambda\log k+\frac{1}{n}h(\lambda)$$

$$\leqslant I(U_J,J;Y_J|L_J)+I(U_J;J;L_J)+H(L_J|U_J)+\lambda\log k+\frac{1}{n}h(\lambda)$$

$$= I(U_J,J;L_J,Y_J)+H(L_J|U_J)+\lambda\log k+\frac{1}{n}h(\lambda)$$

$$= I(U'',L'',Y'')+H(L''|U'')+\lambda\log k+\frac{1}{n}h(\lambda) \tag{3-142}$$

这里，第二个等式成立是因为 U_J 独立于 J。最后，上界对于 U 的大小符合书[10]中的310页。

引理 3.8(定理 3.11 的逆) 对单一信道 W

$$C_{CRI}((V,L),W,R_K,D_1)\leqslant \max_{(V,L,U,X,Y)\in Q*((V,L),W,R_K,D_1)}[I(U;L,Y)+H(L|U)]+R_K \tag{3-143}$$

证明：令 $\{(V^n,L^n)\}_{n=1}^{\infty}$ 是一具有一般 (V,L) 的相关源，W 是一噪声信道，R_K 是Key 率，D_1 符合模型Ⅱ中的失真标准。令 F 和 G 为满足式(3-10)～式(3-12)、式(3-17)以及式(3-14)～式(3-16)的函数。在随机性模型Ⅱ(对于源输出序列长度 n)中，用 X^n 记噪声信道 W^n 的输入。K_n 为发送者根据他自己的相关源的输出以及他的私人随机数确定的无噪声信道的输入。于是，由 Fano 不等式(3-131)成立并且简化成式(3-132)，可得

$$\begin{aligned}
H(F)&\leqslant I(F;G)+n\lambda\log k+h(\lambda)\\
&\leqslant I(F;Y^n,L^n,K_n)+n\lambda\log k+h(\lambda)\\
&= I(F;Y^n,L^n)+I(F;K^n|Y^n,L_n)+n\lambda\log k+h(\lambda)\\
&= I(F;Y^n|L^n)+I(F;L^n)+I(F;K^n|Y^n,L^n)+n\lambda\log k+h(\lambda)\\
&\leqslant I(F;Y^n|L^n)+H(L^n)+H(K^n|Y^n,L^n)+n\lambda\log k+h(\lambda)\\
&\leqslant I(F;Y^n|L^n)+H(L^n)+H(K^n)+n\lambda\log k+h(\lambda)\\
&\leqslant I(F;Y^n|L^n)+H(L^n)+nR_K+n\lambda\log k+h(\lambda)\\
&= \sum_{t=1}^{n}I(F;Y_t|L^n,Y^{t-1})+\sum_{t=1}^{n}H(L_t)+nR_K+n\lambda\log k+h(\lambda)
\end{aligned} \tag{3-144}$$

由式(3-17)可知这里的第二个不等式成立。类似地，由式(3-133)可得

$$\begin{aligned}
0&\leqslant I(F;Y^n,L^n,K_n)-I(F;V^n,L^n)+n\lambda\log k+h(\lambda)\\
&= I(F;Y^n,L^n)-I(F;V^n,L^n)+I(F;K_n|Y^n,L^n)+n\lambda\log k+h(\lambda)\\
&\leqslant I(F;Y^n,L^n)-I(F;V^n,L^n)+H(K_n|Y^n,L^n)+n\lambda\log k+h(\lambda)\\
&\leqslant I(F;Y^n,L^n)-I(F;V^n,L^n)+nR_K+n\lambda\log k+h(\lambda)
\end{aligned} \tag{3-145}$$

注意：这里仅使用了基本的 Shannon 信息测量的性质，以及在假设相关源是无记忆

的情况下，式(3-133)～式(3-136)部分中估计的 $I(F;Y^n,L^n)-I(F;V^n,L^n)$，所有这些都是可得的。于是，这里也有相同的估计结果。

$$
\begin{aligned}
& I(F;Y^n,L^n)-I(F;V^n,L^n) \\
\leqslant & \sum_{t=1}^{n} I(Y_t;V_{t+1},V_{t+2},\cdots,V_n,L_1,L_2,\cdots,L_{t-1},L_{t+1},\cdots,L_n,Y^{t-1},F|L_t) \\
& -\sum_{t=1}^{n} I(Y_t;V_{t+1},V_{t+2},\cdots,V_n,L_1,L_2,\cdots,L_{t-1},L_{t+1},\cdots,L_n,Y^{t-1},F|L_t) \\
& +n\lambda\log k+h(\lambda)
\end{aligned} \tag{3-146}
$$

令 U_j 和 J 如式(3-137)中定义，于是式(3-146) 可重写为

$$
\begin{aligned}
I(F;Y^n,L^n)-I(F;V^nL^n) \leqslant & nI(U_J,J;L_J,Y_J)-nI(U_J,J;V_J,L_J)+ \\
& n\lambda\log k+h(\lambda)
\end{aligned} \tag{3-147}
$$

令 (V'',L'',U'',X'',Y'') 如前面引理所定义，于是式(3-139) 以及 $P_{V''L''U''X''Y''}=P_{VL}P_{U''X''|V''L''}W$ 可实现。由式(3-145)～式(3-147) 可得

$$
0\leqslant I(U'';L'',Y'')-I(U'';V'',L'')+R_K+o(1) \tag{3-148}
$$

同样的方法，如式(3-142)，可以证明

$$
\begin{aligned}
& \sum_{t=1}^{n} I(F;Y_t\mid L^n,Y^{t-1})+\sum_{t=1}^{n} H(L_t)+nR_K+n\lambda\log k+h(\lambda) \\
\leqslant & nI(U'';L'',Y'')+nH(U''\mid L'')+n\lambda\log k+h(\lambda)
\end{aligned} \tag{3-149}
$$

结合式(3-144)，则

$$
\frac{1}{n}H(F)\leqslant I(U'';L''Y'')+H(U''\mid L'')+R_K+n\lambda\log k+h(\lambda)
$$

再次说明，$|u|$ 被限定在支撑引理下，因此证明就完成了。最后，紧跟引理 3.2 和 3.4 的是推论 3.2。

推论 3.2 对于组合信道 W

1)（定理 3.12 的逆部分）

$$
C_{CRI}((V,L),W,D_1)\leqslant \inf_{W\in W}\max_{(V,L,U,X,Y)\in Q((V,L),W,D_1)}[I(U;L,Y)+H(L\mid U)] \tag{3-150}
$$

2)（定理 3.13 的逆部分）

$$
C_{CRII}((V,L),W,R_K,D_1)\leqslant \inf_{W\in W}\max_{(V,L,U,X,Y)\in Q*((V,L),W,R_K,D_1)}[I(U;L,Y)+H(L\mid U)]+R_K \tag{3-151}
$$

3.8 由一般随机性构造水印认证码

R. Ahlswede 和 G. Dueck 在文献[3]中发现：具有相同率的一个认证码通常可以通过发送者和接收者之间的随机性而获得。在一定的条件下，发送者可以以任意小的一个率(Rate)发送一个消息。(指数意义下)

因此，在特定条件下，认证码的容量不比一般随机码的容量小。注意：集合 $Q((V,L),W,D_1)$、$Q^{**}(V,W,R_K,D_1)$、$Q_1((V,L),W,D_1)$ 和 $Q_1^{**}(V,W,R_K,D_1)$ 都不为空。

Steinberg-Merhav 关于具有一通常经验的水印传输码的结果。

为了构建文献[6]中的认证码，Y. Steinberg 和 N. Merhav 引入了一个在发送者和接收者之间建立随机性的传输模拟获得容量范围的一个内界。这个内界对于他们的目标是充分的，下面证明它同样是紧的。

令 $\{V^n\}_{n=1}^{\infty}$ 为一具有字符集 V 的无记忆源。一般地，V 和 W 代表噪声信道，其输入和输出分别为 X 和 Y。函数 (f,g) 被称为具有一仿真失真测度 ρ、失真级 D 和掩饰文档 P_V 的 (n,M,J,δ,λ,D) 水印传输码。如果以下为真

f 是一从 $V^n\times\{1,2,\cdots,M\}$ 到 $\{1,2,\cdots,J\}\times X^n$ 的函数；

g 是一从 $Y^n\times\{1,2,\cdots,J\}$ 到 $\{1,2,\cdots,M\}$ 的函数。

$$\frac{1}{M}\sum_{m=1}^{M}\sum_{v^n\in V^n}P_V^n(v^n)W^n(\{y: g(y^n)=(f_J(v^n,m),m)\}\mid f_X(v^n,m))\geqslant 1-\lambda \tag{3-152}$$

这里，f_X 和 f_J 分别为 f 到 X^n 以及 $\{1,2,\cdots,J\}$ 的投影。

$$\frac{1}{M}\sum_{m=1}^{M}\sum_{v^n\in v^n}P_V^n(v^n)\rho(v^n,f_X(v^n,m))\leqslant D \tag{3-153}$$

对于 $m=1,2,\cdots,M$，存在一子集 $B^m\subset\{1,2,\cdots,j,\cdots,J\}$，其欧式空间 $|B^{(m)}|\geqslant J2^{-n\delta}$，这样，

$$J^{-1}2^{-n\delta}\leqslant P_V^n\{f_J(V^n,m)=j\}\leqslant J^{-1}2^{n\delta} \tag{3-154}$$

对于所有的 j 和

$$\sum_{j\in B^{(m)}}P_V^n\{f_J(V^n,m)=j\}\geqslant 1-\lambda \tag{3-155}$$

g 在这里起着一个解码函数的作用。在接近均匀条件下，式(3-154)和式(3-155)在从通常随机性而来的认证码的构建中起着相同的作用。事实上，可以找到近似均匀条件式(3-16)中更强壮的条件，但出于构建认证码，式(3-154)和式(3-155)已足以满足条件。

一对 (R_1,R_2) 称为在失真 D 级下是可得到的，如果对于所有正实数 δ、λ，均存在一上面定义的 (n,M,J,δ,λ,D) 水印传输码，例如

$$\frac{1}{n}\log M>R_1-\in \tag{3-156}$$

并且

$$\frac{1}{n}\log J>R_2-\in \tag{3-157}$$

可获得的率对称为容量范围并且记为 R。用 $R(*)$ 记作实数对的子集合，这样存在随机数 (V,U,X,Y) 从 $V\times U\times X\times Y$ 取值，$|U|\leqslant|Y|+|X|$，对于 $v\in V,u\in U,x\in X$ 而且 $y\in Y$

$$\begin{aligned}&P_{VUXY}(v,u,x,y)=P_V(v)P_{UX|V}(u,x\mid v)W(y\mid x)\\&E\rho(V,X)\leqslant D\\&0\leqslant R_1\leqslant I(U;Y)-I(U;V)\end{aligned} \tag{3-158}$$

并且，

$$0\leqslant R_2\leqslant I(U;V) \tag{3-159}$$

这在文献[6]中已经证明。

定理 3.20 Steinberg-Merhav。

$$R^* \subset R \tag{3-160}$$

下面证明相反的内在关系成立。

定理 3.21

$$R \subset R^* \tag{3-161}$$

证明：令 (f,g) 为对于足够大的 n，满足式(3-152)～式(3-157)的对函数(这在随后说明)，Z_n、X^n 分别是一在 $\{1,2,\cdots,J\}$ 上具有均匀分布的随机变量。Y^n 是当信道 W^n 输入 X^n 的随机输出。于是，式(3-154)和式(3-155)分别重写为

$$J^{-1}2^{-n\delta} \leqslant P_{Bn|Zn}(j \mid m) \leqslant J^{-1}2^{n\delta} \tag{3-162}$$

对于所有 $j \in B^{(m)}$，并且

$$P_{Bn|Zn}(B_n \in B^{(m)} \mid m) \geqslant 1-\lambda \tag{3-163}$$

因此，

$$\begin{aligned}
&H(B_n \mid Z_n)\\
&= \sum_{m=1}^{M} P_{Z_n}(m) H(B_n \mid Z_n = m)\\
&\geqslant -\sum_{m=1}^{M} P_{Z_n}(m) \sum_{j\in B^{(m)}} P_{B_n|Z_n}(j \mid m)\log P_{B_n|Z_n}(j \mid m)\\
&\geqslant -\sum_{m=1}^{M} P_{Z_n}(m) \sum_{j\in B^{(m)}} P_{B_n|Z_n}(j \mid m)\log J^{-1}2^{n\delta}\\
&= (\log J - n\delta)\sum_{m=1}^{M} P_{Z_n}(m) P_{B_n|Z_n}(B_n \in B^{(m)} \mid m)\\
&\geqslant (\log J - n\delta)(1-\lambda)
\end{aligned} \tag{3-164}$$

这里，由式(3-162)的第二个不等式成立，从式(3-163)可推得第三个不等式，或者等效地

$$\frac{1}{n}\log J \leqslant \frac{\frac{1}{n}H(B_n \mid Z_n)}{1-\lambda} + \delta \tag{3-165}$$

因为 $H(B_n) \leqslant \log J$，式(3-165)意味着：对于一个函数 θ，当 $\delta,\lambda \to 0$，以至于 $\theta(\delta,\lambda) \to 0$，

$$\frac{1}{n}\log J - \theta(\delta,\lambda) < \frac{1}{n}H(B_n \mid Z_n) \leqslant \frac{1}{n}H(B_n) \leqslant \frac{1}{n}\log J \tag{3-166}$$

也就是说，B_n 和 Z_n 是“近似独立的”。进一步，由 Fano 不等式可知 Z_n 独立于 V_n，

$$\begin{aligned}
R_1 - \varepsilon &< \frac{1}{n}\log M = \frac{1}{n}H(Z_n)\\
&= \frac{1}{n}H(Z_n \mid V^n)\\
&\leqslant \frac{1}{n}H(B_n, Z_n \mid V^n)\\
&\leqslant \frac{1}{n}[H(B_n, Z_n \mid V^n) - H(B_n, Z_n \mid Y^n)] + \lambda\log JM + \frac{1}{n}h(\lambda)
\end{aligned}$$

$$= \frac{1}{n}[I(B_n, Z_n; Y^n) - I(B_n, Z_n; V^n)] + \lambda \frac{1}{n} h \log JM + \frac{1}{n} h(\lambda) \quad (3\text{-}167)$$

这里的第二个不等式遵从 Fano 不等式。因为 B_n 是 V_n 和 Z_n 的函数，所以有

$$H(B_n, Z_n \mid V^n) \leqslant H(V^n, Z_n \mid V^n) = H(Z_n) \quad (3\text{-}168)$$

这和式(3-166)遵从于

$$\begin{aligned} R_2 - \varepsilon < \frac{1}{n}\log J &< \frac{1}{n} H(B_n \mid Z_n) + \theta(\delta, \lambda) \\ &= \frac{1}{n}[H(B_n, Z_n) - H(Z_n)] + \theta(\delta, \lambda) \\ &\leqslant \frac{1}{n}[H(B_n, Z_n) - H(B_n, Z_n \mid V^n) + \theta(\delta, \lambda) \\ &= \frac{1}{n} I(B_n, Z_n \mid V^n) + \theta(\delta, \lambda) \end{aligned} \quad (3\text{-}169)$$

至此，我们获得了式(3-167)和式(3-169)中容量的非单一字符特性。后续的证明部分将其简化为单一字符。

首先，分别用 V_n、Y_n 以及 (B_n, Z_n) 代替式(3-128)中的 A_n、B_n 和 C，并且获得

$$\begin{aligned} &H(V^n \mid B_n, Z_n) - H(Y^n \mid B_n, Z_n) \\ &= \sum_{t=1}^{n} [H(V_t \mid V_{t+1}, V_{t+2}, \cdots, V_n, Y^{t+1}, B_n, Z_n) - \\ &\quad H(Y_t \mid V_{t+1}, V_{t+2}, \cdots, V_n, Y^{t-1}, B_n, Z_n) \end{aligned} \quad (3\text{-}170)$$

其次，记 $H(V^n) = \sum_{t=1}^{n} H(V_t)$，因为源是无记忆的，并且 $H(Y^n) = \sum_{t=1} H(Y_t \mid Y^{t-1})$，因此有 $H(V^n) = \sum_{t=1}^{n} H(V_t)$。

$$\begin{aligned} &I(B_n, Z_n; Y^n) - I(B_n, Z_n; V^n) \\ &= H(Y^n) - H(V^n) + [H(V^n \mid B_n, Z_n) - H(Y^n \mid B_n, Z_n)] \\ &= \sum_{t=1}^{n} H(Y_t \mid Y^{t-1}) - \sum_{t=1}^{n} H(V_t) + \sum_{t=1}^{n} [H(V_t \mid V_{t+1}, V_{t+2}, \cdots, V_n, Y^{t-1}, B_n, Z_n) \\ &\quad - H(Y_t \mid V_{t+1}, V_{t+2}, \cdots, V_n, Y^{t-1}, B_n, Z_n)] \\ &= \sum_{t=1}^{n} [H(Y_t \mid Y^{t-1}) - H(Y_t \mid V_{t+1}, V_{t+2}, \cdots, V_n, Y^{t-1}, B_n, Z_n)] \\ &\quad - \sum_{t=1}^{n} [H(V_t) - H(V_t \mid V_{t+1}, V_{t+2}, \cdots, V_n, Y^{t-1}, B_n, Z_n)] \\ &= \sum_{t=1}^{n} I(V_{t+1}, V_{t+2}, \cdots, V_n, B_n, Z_n; Y_t \mid Y^{t-1}) \\ &\quad - \sum_{t=1}^{n} I(V_{t+1}, V_{t+2}, \cdots, V_n, Y^{t-1}, B_n, Z_n; V_t) \\ &\leqslant \sum_{t=1}^{n} I(V_{t+1}, V_{t+2}, \cdots, V_n, Y^{t-1}, B_n, Z_n; Y_t) \end{aligned}$$

$$-\sum_{t=1}^{n} I(V_{t+1},V_{t+2},\cdots,V_n,Y^{t-1},B_n,Z_n;V_t) \tag{3-171}$$

进一步

$$\begin{aligned} I(B_n,Z_n;V^n) &= \sum_{t=1}^{n} I(B_n,Z_n;V_t \mid V_{t+1},V_{t+2},\cdots,V_n) \\ &\leqslant \sum_{t=1}^{n} I(V_{t+1},V_{t+2},\cdots,V_n,B_n,Z_n;V_t) \\ &\leqslant \sum_{t=1}^{n} I(V_{t+1},V_{t+2},\cdots,V_n,Y^{t-1},B_n,Z_n;V_t) \end{aligned} \tag{3-172}$$

因此，令 I 是从集合 $\{1,2,\cdots K,\cdots,n\}$ 均匀取值的随机变量，而且 $U'=(V_{I+1},V_{I+2},\cdots,V_n,Y^{I-1},B_n,Z_n)$ 由式(3-169)～式(3-172)可断定

$$\begin{aligned} R_1-\varepsilon &\leqslant I(U';Y_I \mid I)-I(U';V_I \mid I)+\lambda\log JM+\frac{1}{n}h(\lambda) \\ &\leqslant I(U',I;Y_J)-I(U',I;V_I)+I(I;V_I)+\lambda\log JM+\frac{1}{n}h(\lambda) \end{aligned} \tag{3-173}$$

并且

$$R_2-\varepsilon \leqslant I(U';V_I \mid I) \leqslant -I(U',I;V_I)+\theta(\delta,\lambda) \tag{3-174}$$

令 $U=(U',I)$，$V'=V_I$，$X=X_I$ 和 $Y=Y_I$，于是 $P_{V'}=P_V$，(V',U,X,Y) 形成一马尔可夫链，于是式(3-174)可重写为

$$R_2 \leqslant I(U;V')+\theta(\delta,\lambda) \tag{3-175}$$

并且

$$EP(v',x')<D \tag{3-176}$$

进一步，$I(I,V_I)=0$（因为源是平稳的），而且式(3-173)遵从

$$R_1 \leqslant I(U;Y)-I(U;V')+\lambda\log JM+\frac{1}{n}h(\lambda)+\varepsilon \tag{3-177}$$

最后，$|U|$ 以归一化的方式受支撑定理的约束。

第 4 章 完善隐藏方案

在概率随机分布的条件下,对于给定的明文、消息、掩饰体以及密钥(Key),本章介绍了有关完善隐藏的理论和实现方案,给出了完善保密性和隐藏性的证明,并提出了完善隐密通信算法。

4.1 完善隐藏和完善安全

定义 4.1 如果一个隐密系统 $\Gamma(M,K,C,P_M,P_K,P_C,E,D)$ 满足完善隐藏性、完善解密性以及完善安全性[11],则称 Γ 为完全(Complete)保密的信息隐藏体制。表示如下。

完善隐藏性:对于所有的消息 $m \in M$、$k \in K$ 以及 $c \in X$,存在隐藏函数 $E(\cdot,\cdot)$ 使得 $E(m,k)=c$,并且 $E(m,k)$ 和 c 的分布完全一样,即

$$Pr(E(k,m)=s)=P_c(c) \tag{4-1}$$

完善解密性:对于所有的 $m \in M$ 以及 $k \in K$,存在解密函数 $\Delta(\cdot,\cdot)$,即

$$\Delta(k,E(k,m))=m \tag{4-2}$$

完善安全性:m 的分布独立于 $E(m,k)$,即

$$Pr(m \mid E(k,m)=c)=Pr(m) \tag{4-3}$$

式(4-1)和式(4-2)要求 $\Gamma(g)$ 的隐密过程和解密过程具有一对一的可逆性。式(4-3)则要求隐密后载体的分布和先验的载体具有基本一样的分布,也就是消息的分布和嵌入密信后的载体分布相互独立。

4.2 特征矩阵及其完善性证明

$\Gamma(g)$ 的安全性证明即对完善隐藏性、完善解密性以及完善安全性的证明。首先将 $\Gamma(g)$ 实例化,为此引入一特征矩阵集 $\{H_m\}$,其定义如下。

定义 4.2 特征矩阵集 $\{H_m\}=\{H_m \mid m \in M\}$ 是在已知 m 的情况下,k 和 $E(k,m)$ 的条件概率矩阵,定义为

$$H_m=[H_m(k,c)=P_r(k=\mathrm{k},E(k,m)=c \mid m=\mathrm{m})]_{k\in K,c\in C} \tag{4-4}$$

以后可以看到,矩阵集的定义需要满足 $\Gamma(g)$ 在式(4-1)~式(4-3)中的要求,而且能够覆盖 $\Gamma(g)$ 的所有特性。为此,有以下定理。

定理 4.1 令 $[H_m]=\{(k,s) \mid H_m(k,s)\neq 0\}$ 表示矩阵 H_m 中不为 0 元素的坐标的集合。

(A) 如果元组 (M,K,C,P_M,P_K,P_C,E,D) 为完善隐藏模型,那么

$$\forall m_i,m_j \in M: m_i \neq m_j \rightarrow [H_{m_i}] \cap [H_{m_j}] = \varnothing \tag{4-5}$$

$$\forall m \in M: H_m \times 1^{|C|} = \overrightarrow{P_K} \tag{4-6}$$

(B) 假设元组 (M,K,C,P_K) 以及集合空间为 $|M|$ 的 H_m (其大小为 $|K| \times |C|$),满足式(4-5)以及式(4-6)中的条件,那么下述方案即完善隐藏方案。

函数 $E(\cdot,\cdot)$:输入消息 $m \in M, k \in K$,随机输出 $P_C \rightarrow c$。

这里,$P_C(c) = P_K(k)^{-1} H_m(k,s)$。

函数 $\Delta(\cdot,\cdot)$:输入载体 $c \in X, k \in K$,输出唯一的消息 m。

这里,$H_m(k,s) \neq 0$。

证明　(A):令 $H = (M,K,C,P_M,P_K,P_C,E,D)$,根据对称性可知,给定 k 和 $E(k,m)$ 可唯一确定 m。

$$\forall k, m_i \neq m_j \Rightarrow E(k,m_i) \neq E(k,m_j) \tag{4-7}$$

另一方面,运用反证法,假设 $\forall m_i,m_j \in M: m_i \neq m_j \rightarrow [H_{m_i}] \cap [H_{m_j}] \neq \varnothing$,则

$$\exists k,c: \begin{cases} (Pr(k=k,E(k,m)=c \mid m=m_i) \neq 0) \\ (Pr(k=k,E(k,m)=c \mid m=m_j) \neq 0) \end{cases}$$

$$\Rightarrow \exists k,c: c = E(k,m_i) = E(k,m_j)$$

$$\Rightarrow \exists k: E(k,m_i) = E(k,m_j) \tag{4-8}$$

结合式(4-7)和式(4-8),显然是矛盾的,因此

$$m_i \neq m_j \Rightarrow [H_{m_i}] \cap [H_{m_j}] = \varnothing \tag{4-9}$$

所以,式(4-5)成立。

同时,因为 k 和 m 相互独立,由式(4-4)可知:

$$\begin{aligned} H_m(k,c) &= Pr(k=k,E(k,m)=c \mid m=m) \\ &= Pr(E(k,m)=c \mid k=k,m=m)Pr(k=k \mid m=m) \\ &= Pr(E(k,m)=c \mid k=k,m=m)Pr(k=k) \end{aligned} \tag{4-10}$$

代入式(4-6)得

$$\begin{aligned} (H_m \times 1^{|C|})|_k &= \sum_{c \in C} H_m(k,c) \\ &= \sum_{s \in S} Pr(E(k,m)=c \mid k=k,m=m)Pr(k=k) \\ &= Pr(k=k) \sum_{s \in S} Pr(E(k,m)=c \mid k=k,m=m) \\ &= P_K(k) \end{aligned} \tag{4-11}$$

因此,$H_m \times 1^{|C|} = \overrightarrow{P_K}$,式(4-6)成立。

(A) 证毕。

证明(B):假设式(4-5)和式(4-6)成立,则 $(M,K,C,P_K,\{H_m\})$ 符合 B 中所述的条件。首先,式(4-6)意味着

$$\sum_{k \in K, c \in C} H_m(k,c) = 1 \tag{4-12}$$

令 $H_m(k,c)$ 对应于一概率,即 $H_m(k,c) = Pr(k=\mathrm{k}, a=c \mid m=\mathrm{m})$,这里的 a 等价于 $E(k,m)$。现在要证明的是式(4-3)。从式(4-6)得到

$$Pr(k=k\,|\,m=m)=\sum_{c\in C}Pr(k=k,a=c\,|\,m=m)$$
$$=\sum_{c\in C}H_m(k,c)=(H_m\times 1^{|C|})_k=Pr(k=k) \tag{4-13}$$

因此，k 和 m 相互独立，式(4-3)成立。

同时，由式(4-5)可推断出，至多存在一个 m，使得 $\forall k,s:A_m(k,s)\neq 0,\forall k,s:E(k,m)=s$。

由以上推导可知，对于任意给定的 $k\in K,c\in C$，至多存在一个 $m\in M$ 使得 $E(k,m)=c$，而且从式(4-6)可知，给定 m 和 $P_K(k)\neq 0$，至少存在一个 c 使得 $H_m(k,c)\neq 0$。同时，根据嵌入算法 $E(\cdot,\cdot)$ 的定义可知，若 $E(k,m)=c$，则 $H_m(k,c)\neq 0$。因此，对于任意的 $m\in M$ 和 $k\in K,D(k,E(k,m))=m$。因此，特征矩阵满足对称性。综上所述，$H=(M,K,C,P_K,P_C,E,D)$ 满足完善隐藏性。

4.3 完善保密性和隐藏性证明

定理 4.2 若给定的信息隐藏模型满足对任意 $m\in M$：

$$H_m^{\mathrm{T}}\times 1^{|K|}=\vec{P_c} \tag{4-14}$$

则该模型满足完善安全性和完善隐藏性。

证明：必要性。假设 Γ 满足完善安全性，由式(4-1)和式(4-2)可知

$$(H_m^{\mathrm{T}}\times 1^{|K|})_c=\sum_{k\in K}H_m(k,s)$$
$$=\sum_{k\in K}Pr(\mathrm{k}=k,E(k,m)=c\,|\,m=m)$$
$$=Pr(E(k,m)=c\,|\,m=m)$$
$$=Pr(E(k,m)=c)=P_c(c) \tag{4-15}$$

因此，式(4-14)成立。

充分性：假设式(4-14)成立，根据 A_m 的定义可知：

$$Pr(E(k,m)=c\,|\,m=m)=\sum_{k\in K}Pr(k=k,E(k,m)=c\,|\,m=m)$$
$$=(H_m^T\times 1^{|K|})\big|_c=P_c(c) \tag{4-16}$$

从式(4-16)中可知

$$Pr(E(k,m)=c)=\sum\nolimits_m Pr(E(k,m)=c\mid m=m)Pr(m=m)$$
$$=\sum\nolimits_m P_c(c)P_r(m=m)=P_c(c) \tag{4-17}$$

从式(4-16)和式(4-17)中可知，$E(k,m)$ 独立于 m。因此，Γ 满足完善保密性。同时，由式(4-17)可知，式(4-1)成立。因此，Γ 满足完善隐藏性。

推论：令 Γ 是具有完善隐藏性以及与消息的分布相互独立，于是 Γ 被认为是完善安全的。

证明：假设 Γ 具有完善隐藏性，从式(4-1)可得

$$P_c(c) = Pr(E(k,m) = c) = \sum_m Pr(E(k,m) = c \mid m = m) Pr(m = m)$$
$$= \sum_m \sum_k Pr(k = k, E(k,m) = c \mid m = m) Pr(m = m)$$
$$= \sum_m \sum_k H_m(k,c) Pr(m = m)$$
$$= \sum_m Pr(m = m)(H_m^T \times 1^{|K|})|_c \tag{4-18}$$

因为对于所有 $m \in M$，并且 m 与 $k \in K$ 独立，因此有 $\sum_m P_r(m = m) = 1$，于是

$$P_c(c) = (H_m^T \times 1^{|K|})|_c \tag{4-19}$$

满足式(4-14)，意味着 Γ 是完善安全的。

有关 H 方案中矩阵集 $\{H_m\}$ 的构造算法如下。

算法 4.1

输入　整数 $c_1, c_2, \cdots, c_n$

输出　整数 k 和 $|M|$ 个大小为 $k \times n$ 的矩阵 $H_1, H_2, \cdots, H_m$

如果 $\forall i \in \{1,2,\cdots,n\}$：$c_i = 0$，于是

　　$H_1, H_2, \cdots, H_m \Leftarrow$ 空矩阵

　　$k \Leftarrow 0$

否则 $Q \Leftarrow (c_1 + c_2 + \cdots + c_n)/m$

　　σ 是 $(1,2,\cdots,n)$ 的一个排列，以使 $c_{\sigma 1} \geqslant c_{\sigma 2} \geqslant \cdots \geqslant c_{\sigma_n}$

　　$\delta \Leftarrow \min(Q - c_{\sigma_{m+1}}, c_{\sigma_m})$

对于 $i \in \{1,2,\cdots,m\}$，$c'_{\sigma_i} \Leftarrow c_{\sigma_i} - \delta$

对于 $i \in \{m+1, m+2, \cdots, n\}$，$c'_{\sigma_i} \Leftarrow c_{\sigma_i}$

　　$H'_1, H'_2, \cdots, H'_m, k' \Leftarrow$ 算法后的 $(c'_1, c'_2, \cdots, c'_n)$

　　$k \Leftarrow k' + m$

对于 $i = 1:m, j = 1:m$，

　　$t \Leftarrow ((i+j) \bmod m) + 1$

　　把单位行矩阵 δe_{σ_t} 添加给 H'_i

结束　$H_i \Leftarrow H'_i$

算法 1 是特征矩阵的生成算法。其中 $\{P_{C_1}, P_{C_2}, \cdots, P_{C_n}\}$ 表示原始载体的统计分布，将 $\{P_{C_1}, P_{C_2}, \cdots, P_{C_n}\}$ 中各项通过通分化为整数 $\{c_1, c_2, \cdots, c_n\}$ 后，作为算法 1 的输入。运行结果的输出为密钥空间 $|K|$ 和 $|M|$ 个 n 维的特征矩阵，其中每行的长度为 $|K|$。

4.4　完善隐密通信算法

4.4.1　相关概念的定义

隐密通信技术的目的是验证秘密数据的不可抵赖性和完整性。基于完善隐藏模型，本章提出一种完善密钥隐密通信系统。发送方利用密钥 k 把机密信息 m 隐藏到载体内，

通信接收方采用共享密钥 k 能够逆向从隐密载体 s 中检测出机密信息，k 可以看作是将秘密信息实施加密或者是处理嵌入操作的密钥，但这样的隐密通信系统基于一个假设，即能够经过安全的信道传送密钥。

引入不确定性因素的信息隐藏系统增加了载体选择的随机性，使得真正嵌入消息的载体 C 是从字符集 C_S 中选取而来，即 $C\subseteq C_S$。同时，根据 4.2 节的分析可知，假设隐藏消息前后载体的统计特性不发生改变，那么完善隐藏模型可以满足理论意义的安全性。因此，完善隐密通信系统基于这两种分析定义具体通信流程。

定义 4.3 频数向量。

频数向量 $F=\{f_1,f_2,\cdots,f_n\}$，f_i，$i=1,\cdots,n$，表示第 i 个载体样本 C_{Si} 在实验中被选取并用于隐藏秘密信息的次数。

定义 4.4 载体分布。

$$\forall c\in C_S, P_c(c)=f_i(c)/\sum_{i=1}^{n}f_i, P_c(c)\leqslant\frac{1}{|M|} \tag{4-20}$$

由载体分布的定义可知

$$P_c(c)\leqslant\frac{1}{|M|} \tag{4-21}$$

当载体空间 $|C_S|$ 与秘密信息空间 $|M|$ 的大小一样时，式(4-21)中的等号成立。由此说明，在实际嵌入过程中，载体有一定的冗余，冗余量大小为 $|C_S|-|M|$，实际载体空间为 $|M|$。嵌入秘密信息的载体集合为载体字符集的子集，符合不确定性安全分析模型。

4.4.2 数据预处理

因为完善隐密通信假设通信双方可通过安全信道传递秘密信息，所以背景知识共享可以通过密钥传递实现。而特征矩阵的建立主要通过载体的频数向量和分布实现。

假如给定载体的分布为 $P_c=(P_{c_1},P_{c_2},\cdots,P_{c_n})$，通过算法 1 建立的特征矩阵如下。

$$A_{m_1}=\begin{bmatrix}P_{c_1}&0&\cdots&0\\0&P_{c_2}&\cdots&0\\0&\cdots&P_{c_3}&0\\\cdots&\cdots&\cdots&\cdots\\0&0&\cdots&P_{c_n}\end{bmatrix}\quad A_{m_2}=\begin{bmatrix}0&P_{c_2}&\cdots&0\\P_{c_1}&0&\cdots&0\\0&\cdots&0&P_{c_3}\\\cdots&\cdots&\cdots&\cdots\\0&\cdots&P_{c_n}&0\end{bmatrix},\cdots,$$

$$A_{m_n}=\begin{bmatrix}0&0&\cdots&P_{c_3}\\0&\cdots&P_{c_n}&0\\0&P_{c_2}&\cdots&0\\\cdots&\cdots&\cdots&\cdots\\P_{c_1}&0&\cdots&0\end{bmatrix}$$

从特征矩阵 A_m 中可以看出，每一行每一列只有一个矩阵元素不为 0，符合完善隐藏模型的对称性；每一列元素的和与对应载体的分布相等；每一行元素的和对应密钥的分布。因为隐密通信具备一定的实时性，当每次获取不同的通信密钥时，通过特征矩阵选取

的载体也会适应性地发生改变。图 4-1 显示了不同密钥作用下，秘密信息与载体之间的对应关系。

从图 4-1 可以看出，在不同密钥的作用下，秘密信息被映射嵌入不同的载体中，从而实现载体的实时性，保持其新鲜性，这是隐密通信特征的重要体现。数据预处理使得发送方能够随机选择载体，而不是在同一载体中的相同位置重复嵌入。当攻击者根据之前的隐密载体进行学习时，并不会影响后续通信的安全进行，体现了载体选择的独立性。同时，隐密通信还能够根据载体的不同分布得到不同特征矩阵，使得载体的选择能够根据载体分布的变化以及载体内容的改变而改变。数据库建立操作使双方通信能够更加安全，也是通信的关键所在。

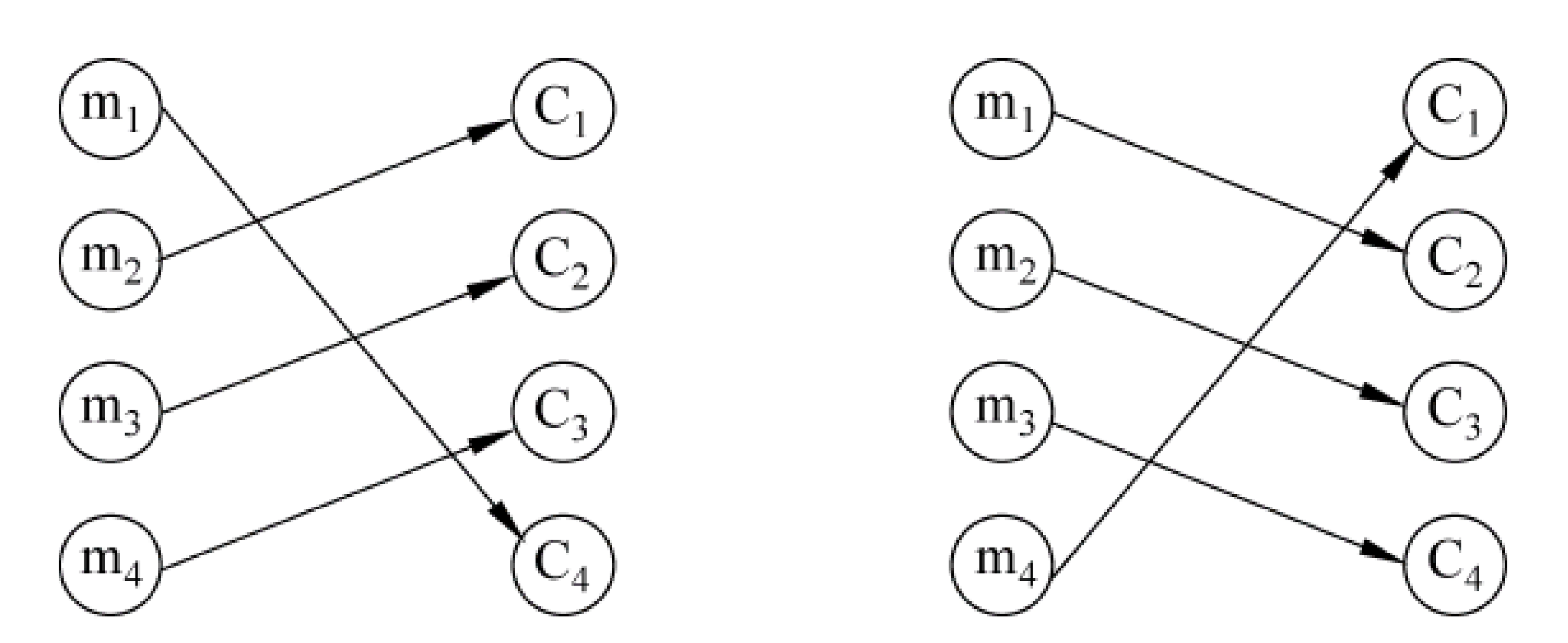


图 4-1 不同密钥情况下，秘密信息与载体之间的对应关系

4.4.3 秘密信息嵌入及提取算法

通信双方根据已了解的数据建立隐密通信的特征矩阵，并利用对称密钥发送和提取秘密信息。具体嵌入流程可归纳如下。

(1) 发送方 Alice 和接收方 Bob 进行隐密通信之前，双方利用密钥 k 共享数据 C，通过数据预处理操作创建特征矩阵。

(2) Alice 选取临时密钥 k，获取 A_m 中 $A_m(k,c) \neq 0$ 的元素对应的载体 c。

$$A_m(k,c) \neq 0 \rightarrow c \tag{4-22}$$

(3) Alice 选取载体 c 中特征比较明显的区域嵌入秘密信息，得到隐密载体 s。

$$E_k(m \in M, c \in C) = s \tag{4-23}$$

(4) Alice 把获得的隐密载体 s 经过不受怀疑的信道发送给 Bob。

Alice 通过保持载体的实时性，并在载体特征明显的区域隐藏信息后，使得隐密载体满足不可感知性、鲁棒性和安全性，从而能够在公开信道中安全地与 Bob 进行通信。

隐密通信的提取操作是嵌入操作的逆操作，主要流程可归纳如下。

(1) Bob 进行隐密通信之前，利用密钥 k 共享数据 C，通过数据预处理操作创建特征矩阵。

(2) Bob 使用密钥 k 和获取到的隐密载体 s，根据特征矩阵中 $A_m(k,s) \neq 0$ 的对象抽取消息 m。

$$D_k(A_m, s) = m \tag{4-24}$$

图 4-2 描述的是隐密通信的整体流程。

其中，对秘密信息的加密操作属于可选环节，若进行加密，则接收方需要进行相应的

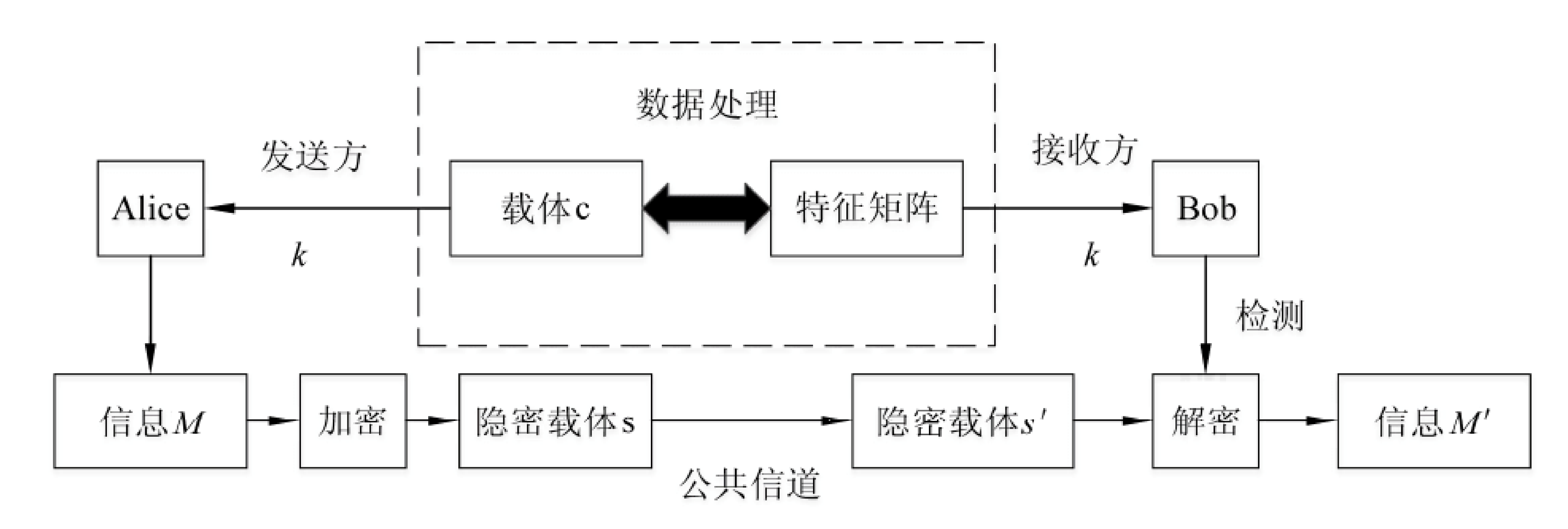


图 4-2　隐密通信的整体流程

解密操作。

4.4.4　完善隐密算法的安全性分析

定义 4.5　对于一组给定的消息 $M=\{m_1,m_2,\cdots,m_l\}$，$C=\{c_1,c_2,\cdots,c_L\}$，$C\subset C_S$ 为原始载体，令 $\hat{C}=\{\hat{c}_1,\hat{c}_2,\cdots,\hat{c}_L\}$，$\hat{C}\subseteq C_S$ 为攻击者模仿攻击所选择的特征序列。其中，L 为可能的候选载体大小；l 为实际选中的隐密载体大小，$l\leqslant L$；$L-l$ 即为算法提供的冗余信息。

在给定 M 的前提下，条件互信息可定义为

$$I(C,\hat{C}\mid M)=\sum P(C,\hat{C}\mid M)\cdot\log\frac{P(C,\hat{C}\mid M)}{P(C\mid M)P(\hat{C}\mid M)}\tag{4-25}$$

原始载体特征与攻击的特征之间的互信息可定义为

$$I(C,\hat{C})=\sum_{M^l\subset M}P(M)\cdot I(C,\hat{C}\mid M)\tag{4-26}$$

联合概率分布 $P(\hat{C},M)$ 可以用相应的条件概率表示为（$c_i'\in C$）

$$P(\hat{C},M)=P(M)\cdot\prod_{i=1}^{L}P(\hat{c}_i\mid c_i',m_i)\tag{4-27}$$

差异化函数定义为

$$D(P(C,M),P(\hat{C},M))=\sum_{C,M}P(C,M)\cdot\log\frac{P(C,M)}{P(\hat{C},M)}\tag{4-28}$$

假设隐密算法是公开的，对于合法用户而言，为了防止秘密信息泄露的最优策略是要让隐密前后的载体之间的条件互信息最大，即式(4-25)中的互信息最大，此时算法提供的模糊性最强。

相反，对于攻击者来说，破解算法的最优策略是：尽力搜索到一个概率分布，使隐密前后特征序列的差异最小化，即使式(4-28)中的差异化函数达到最小值。

将式(4-27)代入式(4-28)，则

$$D(P(C,M),P(\hat{C},M))=\sum_{C,M}P(C,M)\cdot\log\frac{P(C,M)}{P(\hat{C},M)}$$

$$= \sum P(C,M)\log \frac{P(C,M)}{P(M)\cdot \prod_{i=1}^{L} P(\hat{c}_i \mid c_i, m_i)}$$

$$= \sum P(C,M)\log \frac{P(C,M)}{P(M)} - \sum P(C,M)\sum_{i=1}^{L}\log \frac{P(c_i,\hat{c}_i,m_i)}{P(\hat{c}_i \mid c_i,m_i)} \tag{4-29}$$

为了分析方便，把 C 分解为两部分，嵌入消息的部分 $r(i)\neq 0$ 以及 $r(i)=0$ 没有改变的部分，那么式(4-29)可表示为

$$\begin{aligned} D(P(C,M),P(\hat{C},M)) &= \sum P(C,M)\cdot \log \frac{P(C,M)}{P(M)} \\ &= \sum P(C,M)\cdot \log \frac{P(C,M)}{P(M)} \\ &\quad - \sum P(C,M)\cdot \sum_{i=L-l}^{L} \log P(c_i \mid m_i) \\ &\quad - \sum P(C,M)\cdot \sum_{i=1,r(i)\neq 0}^{l} \log \frac{P(c_{r(i)},\hat{c}_i \mid m_i)}{P(c_{r(i)} \mid m_i)\cdot P(\hat{c}_i \mid m_i)} \end{aligned} \tag{4-30}$$

式(4-30)中第一个加数对于特定的消息组来说是一个常量，第二部分是冗余信息，最后一部分会受到信息匹配程度的影响，因此最小化差异 D 相当于最大化公式(4-30)中的第三部分。

$$\begin{aligned} &\max\left(\sum P(C,M)\sum_{r(i)\neq 0,i=1}^{l} \log \frac{P(c_{r(i)},\hat{c}_i \mid m_i)}{P(c_{r(i)} \mid m_i)P(\hat{c}_i \mid m_i)}\right) \\ &= \max\left(\sum_{r(i)\neq 0,i=1}^{L}\sum P(M)\sum_{r(i)\neq 0,i=1}^{l} P(c_{r(i)},\hat{c}_i \mid m_i)\cdot \log \frac{P(c_{r(i)},\hat{c}_i \mid m_i)}{P(c_{r(i)} \mid m_i)P(\hat{c}_i \mid m_i)}\right) \end{aligned} \tag{4-31}$$

通过条件交互熵简化公式可得

$$\max\left(\sum_{r(i)\neq 0,i=1}^{L}\sum P(m_i)\cdot I(c_{r(i)},\hat{c}_i \mid m_i)\right) = \max(I(C,\hat{C})) \tag{4-32}$$

从上述公式推导可知，对于合法接收者，由于接收者与发送者共享密钥，她/他能够准确地从隐密信道中解码出正确消息。也就是说，在知道密钥的情况下，$c_{r(i)}$ 和 $\hat{c}_i$ 唯一匹配，此时差异化函数回归常数。

当 $L=l$ 时，意味着 $|M|=|K|=|C|$。从攻击者的角度分析可知，假设采用 LSB 算法实现通信，攻击者能够成功提取秘密信息的可能性为 $1/2^L$。随着 L 的增大，攻击者能够成功提取秘密信息的概率将呈线性下降趋势，公式中的互信息将越来越小，模拟序列与隐藏序列的差异化越来越大；当 $L>l$ 时，从 L 中选取 l 项是通过密钥进行挑选的。攻击者首先要排除冗余部分 $(L-l)$项带来的干扰，对于她/他而言，当密钥是通过安全信道传输时，系统将依赖于密钥的安全性。因此，系统的安全性符合 Kerckhoff 的安全理论：密钥是确保系统安全性的唯一关键因素。

对发送者而言，使得式(4-30)最大化即互信息最大是她/他能采取的最佳策略。此

时，原始序列和隐密后的序列之间的统计分布十分接近，当二者完全相同时，系统将达到理论绝对安全，如图 4-3 所示。

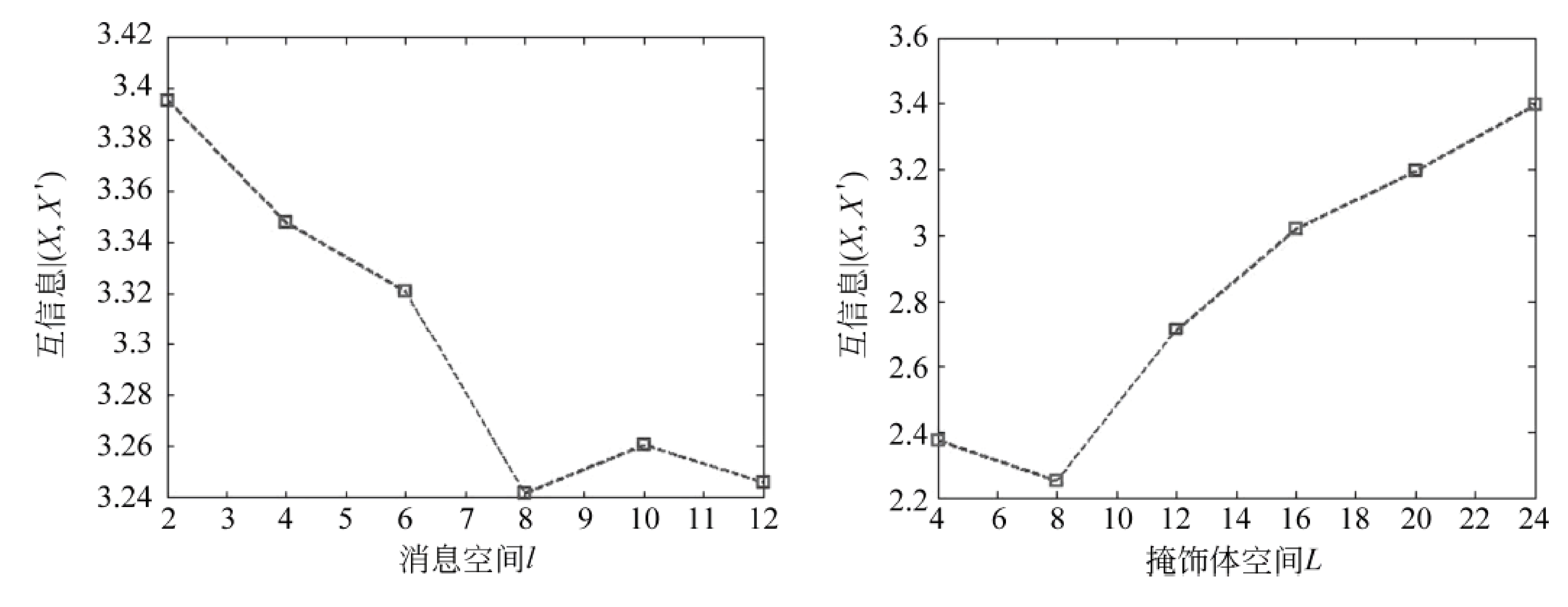


图 4-3　互信息与 l 及 L 之间的关系

为了显示互信息大小与消息空间大小之间的关系以及互信息大小与载体空间大小之间的关系，实验通过伪随机数产生器模拟载体的 F，构建隐密通信模型。当载体空间一定（$L=24$），而消息空间大小不确定时，交互信息的大小如图 4-3(a)所示。当消息空间大小一定（$l=16$），而载体空间不确定时，交互信息的大小如图 4-3(b)所示。

从图 4-3 中可以看出，当载体中隐藏相对于 L 越少的消息时，隐密前后载体之间的互信息越大，二者的统计特性越接近，系统整体达到的效果最佳。

从图像的角度分析该问题，将整幅图像看做候选载体集合，其空间大小为 L，通过密钥控制，从 L 中选取 l 个载体作为隐密载体集合进行隐密。那么，对于攻击者来说，她/他面临的就是要从 L 中甄别出（$L-l$）个冗余项。

4.4.5　算法的应用及结果分析

完善隐密通信模型与一般信息隐藏模型主要有 3 点区别：首先，完善隐密通信模型中嵌入载体的选择是通过完善隐藏算法生成并选取的，而一般隐密通信模型是固定嵌入事先获取的原始载体中；其次，完善隐密通信模型包含载体字符集 C_S，使得载体 $C\subseteq C_S$，当使用不同密钥 k 进行通信时，C 也会相应地变化，增大了载体的随机性和实时性。在经典隐藏模型中，密钥 k 仅作为加密或者嵌入密钥，并不影响载体的选择；最后，在完善隐密通信中，载体与秘密信息之间的对应关系是通过完善隐藏特征矩阵置乱的，同一秘密信息在不同密钥的作用下会被隐藏到不同的载体中。在经典隐藏模型中，秘密信息按序嵌入原始载体中，并且不会因为密钥的改变而发生变化。

图 4-4 显示了不同密钥作用下，系统选取进行秘密信息隐藏的载体的情况（载体空间大小为 24，秘密信息空间大小为 16）。

图中正方形区域表示候载体集合，三角形区域标识的是通过密钥选取的真正进行消息隐藏的载体。

从图 4-4 可以看出，当密钥发生变化时，载体集合中的元素本身及载体的顺序均发生






图 4-4　不同密钥作用下载体位置的变化情况

变化，并且具有很少的重复性。一般信息隐藏模型是在载体的固定位置进行嵌入，因此它不具备随密钥变化而变化的实时性。

图 4-5 是分别采用隐密通信方案和文献[12]的方案在 lena 图像中进行 3 次秘密信息嵌入后的效果图。


(a) 文献[2]嵌入信息后的图像


(b) 本文算法嵌入信息后的图像

图 4-5　不同算法嵌入信息效果图

其中，秘密信息的大小为 256 bits，拉伸系数为 0.4，在图像的 DCT 变换域实现隐藏。两幅图像从视觉上无法感知到太大的差别，可以通过计算图像的均方差(Mean Squared Error，MSE)进行比较。计算公式如下。

$$\mathrm{MSE} = \frac{1}{M \times N} \sum_{0 \leqslant i \leqslant N} \sum_{0 \leqslant j \leqslant M} (px_{ij} - px'_{ij})^2 \tag{4-33}$$

其中，M 和 N 分别指载体的长和宽；px_{ij} 表示原始载体的像素值；px'_{ij} 表示隐密后载体的像素值。

还可以通过获取峰值信噪比(Peak Signal to Noise Rate，PSNR)进行分析，计算公式

如下。

$$\mathrm{PSNR} = 10 \times \log_{10} \frac{L \times L}{\mathrm{MSE}} \tag{4-34}$$

L 表示载体像素的最大灰度值，一般采用 $L = 255$。

经过计算，图 4-5(a) 中 PSNR＝44.10，图 4-5(b) 中 PSNR＝64.67。因此，当在同一载体中进行多次重复嵌入时，完善隐密通信的效果更好，PSNR 越大，失真越少。这是因为，当进行重复嵌入时，完善隐密通信根据每次的密钥选择不同的位置嵌入，而文献[2]是在固定的位置进行嵌入。当嵌入位置比较分散时，会将加入的信号量分散，而不是集中在一起，进而能够较好地保持图像质量。

水　印　篇

本篇围绕数字认证和数字追踪技术，主要介绍作者在数字认证和版权保护方面的最新研究成果。这部分内容主要集中在第5～9章中讲述。其中，第5章详细论述数字水印技术的相关知识；第6章介绍水印在数字多媒体产品保护中的应用；第7、8章分别介绍数字水印技术在图像和视频方面的设计方案；第9章介绍在自然语言文本中的隐藏算法。

第 5 章 数字水印技术

以数字媒介为载体的产品(如数字影院、图书馆、音乐、图像和视频等)由于其获取容易、复制简单和传播迅速等优点,极大地推动了信息的普及和交流。但正如人们看到的,利用网络的开放性和共享性进行的诸如侵犯、滥用版权、产品剽窃以及篡改重发等大量的恶意行为,严重损害了数字产品的创作者和使用者的正当利益。因此,迫切需要新的技术手段保证数字产品的真实性和完整性。本章着重介绍数字水印的相关技术,后续章节再探索其在多媒体产品版权保护中的应用。

5.1 密码学、信息隐藏和数字水印

以往,有关版权保护技术已有很多成果,但大多数涉及的是使用密码学中的加密或者其他基于密码学的类似技术。对于今天的人们,加密和解密已不再具有神秘性,已成为大家生活中经常使用的技术之一,密码学是保护数字产品内容常见的,也是发展得较为完善的一种保密技术。一个典型的例子:在发送数字产品之前对其内容进行加密,仅把密钥给予那些购买了产品内容的合法用户,但遗憾的是,通过加密并不能帮助销售者监视合法用户如何处理解密后的内容。也就是说,加密只保护传输中的内容,而内容一旦被解密,就不再有保护的作用了。可以看出,尽管密码学在保护公共及个人信息的安全方面起着重要的作用,而且也能够帮助解决数字产品版权保护中相关的一些问题,但在新的应用背景和条件下,单靠密码学的技术是不够的。

国内外许多学者提出了一系列新的信息安全的思想,信息隐藏(Information Hiding)便是当前得到热烈讨论的技术之一,其基本意思是,将一种信息隐藏于另一种信息中,这里所说的另一种信息必须能够为待隐藏的信息构成一个足够复杂而且不易察觉的信息环境。信息隐藏技术涉及的学科门类比较繁多,Petitcolas F. A. P. 等对该技术涉及的内容进行了较详细的概括并进行了分类[13],如图 5-1 所示。信息隐藏其实是一门古老的学科,无论从其定义,还是从实现原理上都容易理解,其思想可以追溯到古希腊的隐密术(Steganography)[13-15]。

数字水印(Digital Watermarking)是信息隐藏中的重要技术之一,它和密码学以及信息隐藏的其他学科领域紧密相关,许多具体技术方法可以相互共享,其定义可理解为:不被感知的在数字产品(Digital Product)中嵌入信息的处理行为。数字水印技术和传统的密码学方法不同,它是依据信息隐藏的思想将重要的、可认证的信息嵌入图像、视频、音频及文本文件等数字多媒体的内容中,成为难于感知的部分,但表面上并不影响产品的可视

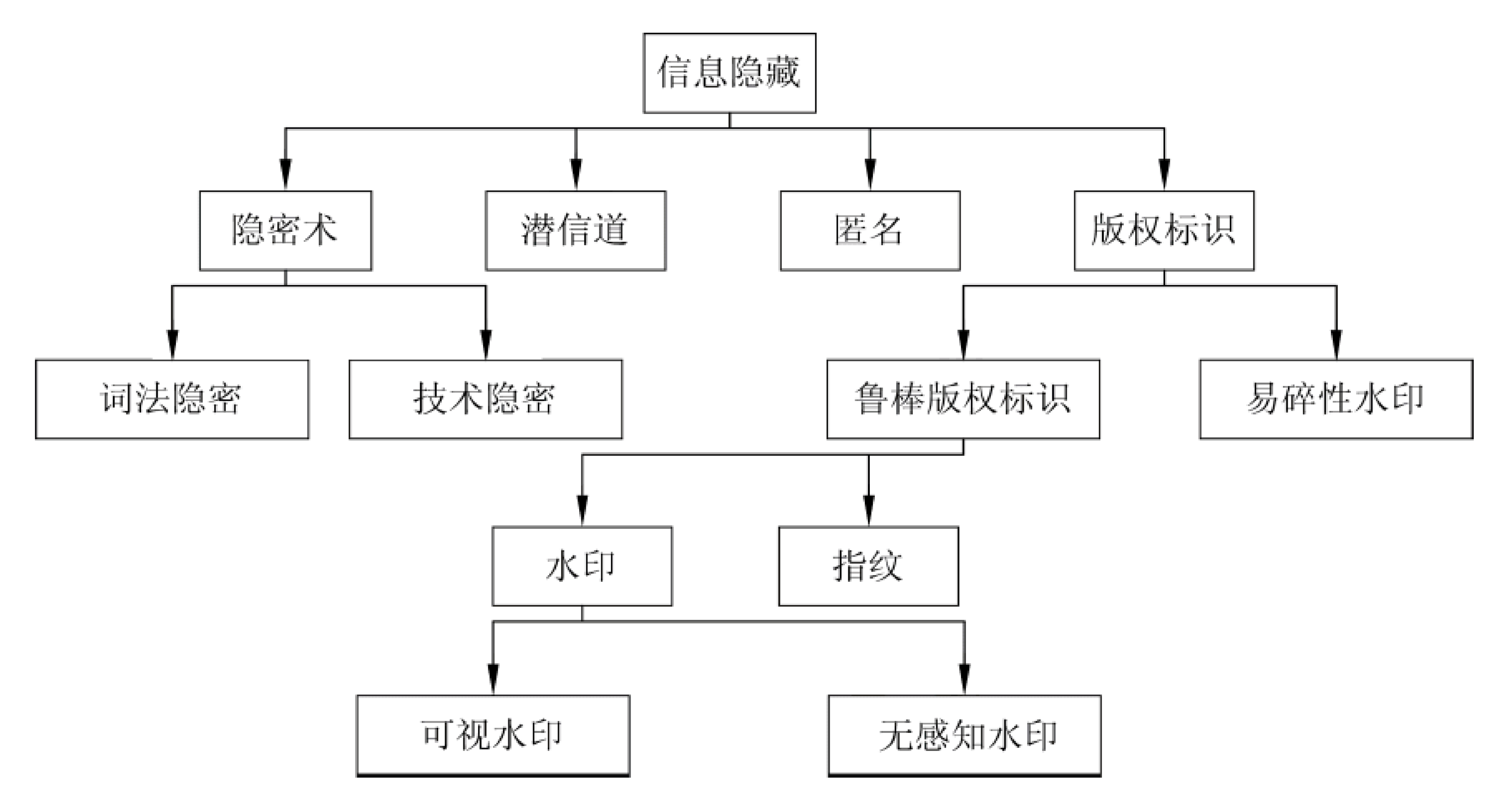


图 5-1　信息隐藏技术分类

(可读/听)性,而一旦需要,则可以从加了水印的产品中检测出预先嵌入的信息,对产品的完整性以及版权进行认证和证明,以防止对产品的篡改和盗版。嵌入的水印信息甚至还可以作为各种多媒体播放器的有条件进入的控制信号,阻止那些没有得到合法授权的团体或个人对产品的复制和滥用,从而达到对多媒体产权的跟踪和保护[16-18]。所以,正是数字产品的知识产权保护及其他一系列迫切需求导致数字水印诞生,数字水印技术已经被认为是解决多媒体数字版权的有效工具之一。

5.2　数字水印技术的分类

水印的分类各种各样,从水印本身抗信号处理以及几何失真的性能角度,可以将水印分为鲁棒水印(Robust Watermarking)和脆弱水印(Fragile Watermarking);从所保护的多媒体对象分类,也可以将水印分为语音水印、文本水印、图像水印和视频水印等;其他分类这里不再列举。

5.2.1　脆弱水印和鲁棒水印

有关鲁棒和脆弱的水印技术是目前主要研究的两类不同的水印技术。下面对这两种不同性质的水印概念加以描述和区分。

1. 脆弱水印

脆弱水印对任意发生在宿主信号中的修改都具有很高的敏感度,将它应用于多媒体数据作为一个整体,可用来保护其完整性。这种水印的特点是:在多媒体中嵌入的信息量很小,也就是说,在多媒体中一旦存在较小的变化,就足以破坏加入的水印信息,而通过对变化了的水印的提取及分析,可对原始多媒体本身经历的变化进行测定和评估,进一步对多媒体数据的完整性、内容的真实性等进行鉴定或认证[19-22]。针对不同的应用,用于认证的水印又可细分为脆弱水印和半脆弱(Semi-Fragile)水印。半脆弱水印主要用于多

媒体数据的内容认证。一方面，对于一些数据处理操作，如轻度的 JPEG 压缩等，多媒体数据的内容并没有发生实质性的改变，其质量仍是可以接受的；另一方面，压缩编码等操作又经常是减少数据存储量和传输量所必需的，因此要求半脆弱水印对可以接受的多媒体数据处理操作必须是鲁棒的，而对其他处理则能够进行检测并加以区分，脆弱和半脆弱这两种水印的应用区别主要是衡量数字产品可以接受变化的程度。

保护原始产品的完整性和真实性，从而不被其他非授权的机构或个人篡改而挪为商业的非法应用。脆弱水印是目前解决这类问题的有效手段之一。

2. 鲁棒水印

鲁棒水印根据其感知性可以分为两类：可视水印[23-29]和不可感知水印[30-37]。类似于传统的纸质货币的水印，可视水印的主要目的是将注册的版权明确化，防止其他团体或个人冒充或非法使用。比较常见的诸如数字文档上加载的半透明图标、商业广告以及电视台在它们频道上播放节目附加的台标等，可视水印一般不影响数字产品的视觉效果和正常使用。可视水印的典型运用是在 IBM 数字图书馆项目中[38]，这一研究成果已被美国国会图书馆等几所著名图书馆采用。不可感知水印一般指在多媒体数据中嵌入秘密的信息，而不造成人类感觉上失真的这种情形，这种水印技术在保护数字产品的知识产权方面起主要作用。例如，作者版权遭到侵犯时，可以为第三方提供证据，告诉谁是真正的版权所有者；打击盗版时根据盗版媒体提取出的水印可以跟踪非法复制的用户和盗版来源。水印的“鲁棒性”取决于实际的应用。一般来说，在保留数字产品的使用价值的前提下，鲁棒水印能够抵抗一定程度的数字处理技术，如有损压缩、滤波、缩放、旋转、裁剪等常用操作带来的破坏。此外，鲁棒水印还必须能够抵制各种方面的蓄意攻击。

在构成多媒体产品版权的永久性保护方面，往往需要考虑使用鲁棒性高的水印技术。

5.2.2　宿主媒体不同的水印技术

1. 数字图像水印技术

数字图像水印是多媒体水印的一个重要分支，目前有关图像水印提出的方案比较多，简单概括为以下 3 个类型。

- 基于空间域的水印技术：最早的关于图像水印的文献发表于 1993 年，Caronni 提出了完整的跟踪图像非法传播的系统[39,40]。他建议用空变信号调制对图像进行标示并把这一过程命名为标记（Tagging）。同年，Tirkek 等人也提出了一些数字图像水印的方法和思想[41]，他们同样强调了图像水印的重要性并提出了一些新的应用，包括标记、版权保护、图像数据的访问控制、防伪保护等。将水印信息调制在图像像素的最不重要比特（LSB）或者最不重要的几个比特中，该类水印技术的缺点是鲁棒性较差。为提高水印在空间域的鲁棒性，此后出现了一些更复杂的技术。Hernandez 等人提出了一种深度 2D 多脉冲幅度调制的方法[42]。Wolfgang 等人把二维的 m 序列嵌入图像的 LSB 平面[43]，并利用互相关函数改善了检测过程。利用图像像素的统计特性，一种方法是把图像像素分成两个集合，通过修改两个集合的均值差嵌入水印。这种方法对 JPEG 压缩具有较好的鲁棒性。

利用人类视觉系统的特性，Macq 等人提出了一种使用伪装和调制的水印方法[43-45]，使嵌入的水印信号更加适应于载体图像。Kutter 等人提出一种更加复杂的感知模型[46,47]，在分析人类视觉系统的伪装特性以及水印信号本身特性的基础上推导出一种优化的 HVS 加权函数，用于亮度和蓝色通道水印的嵌入。Chen 等人提出了一种基于量化索引调制，而不是扩频调制的水印嵌入方法[48]，并宣称其性能优于基于扩频调制的水印方法。此外，空域水印还可以通过修改图像的几何特征和利用分形图像编码实现[49-51]。为了抵制几何失真，Nikolaidis 等人提出一种空间域水印方法[52,53]，他们对图像中的重要区域进行鲁棒性的估计和分割并且在这些区域嵌入水印信息。

- 基于频率域的水印技术：相比于空间域的水印技术，在频率域嵌入水印通常具有很多优势。Koch 等人提出了基于 DCT(离散余弦变换)域的水印方法，通过修改伪随机选定的中频系数对的差值嵌入水印[54]。Tao 等人提出一种自适应 DCT 域的水印技术，把图像块按照噪声敏感特性分为 6 个级别，每一级别嵌入不同强度的水印[55]。Cox 等人提出将水印嵌入图像中感知重要的区域中，其思想是，要破坏水印，必然要破坏图像的重要内容[56]。为了得到水印的鲁棒性和不可感知性的最佳折中，Zeng 等人提出一种基于感知模型的变换域图像自适应水印方案，用临界可见误差(Just Noticeable Difference，JND)确定水印的最大嵌入能量[57-59]。Hernández 等人结合视觉模型提出一种 DCT 域盲水印技术，对 DCT 系数统计建模并设计了一种最大似然比水印检测器[60]。类似的水印技术还被引入离散小波变换(DWT)域中。利用小波变换的多分辨特性，嵌入的水印在不同分辨层上具有不同的鲁棒性和视觉特性。与 DCT 比较，小波变换具有更好的能量集中特性，其良好的时-频分解特性更符合人类视觉系统的特点，因此被新一代的压缩标准(如 MPEG-4 及 JPEG-2000)所采用[51]。Kundur 等人提出一种基于多分辨信息融合的 DWT 域水印技术[21,62,64]。Xia 等人提出在载体图像的每个分辨层上嵌入水印以及分层的检测方法[64]。Zhu 等人基于二维和三维离散小波变换提出了一种图像和视频水印的统一方法[65]。Swanson 等人利用时域小波变换并结合频率掩蔽特性，提出了一种多分辨视频水印[66]。Barni 等人把感知模型精确到每个图像小波系数[67]，从而最大程度地提高了水印能量。还有一大类水印技术基于离散傅里叶变换(DFT)域[68-70]、Radon-Wigner 域[71]等。利用 DFT 的缩放和旋转不变特性，这一类变换域水印对几何失真能够实现较好的鲁棒性。
- 基于信息理论的水印技术：一些学者利用通信和信息论的知识探讨了数字水印的嵌入策略和容量问题。Hernandez 等人从通信系统的观点出发，理论分析了在加性噪声干扰、裁剪、线性滤波等失真情况下，隐藏信息的误码率以及特性变化[72]。Servetto 等人把图像水印看作高斯信道环境中极低信噪比的信号传输和检测过程，推导了以噪声方差为参数的图像加性水印的容量[73]。Môulin 利用香农的经典通信理论推导了数字水印的通用框架[74]，分析了无记忆并行高斯模型下的水印信道容量，并讨论了利用边缘通信进行盲解码的思想。Su 等人去掉了水印信道模型中的无记忆假设，并讨论了线性滤波和加性噪声下的最佳嵌入策

略[75]。Pérez-González 等人利用香农理论讨论了信道编码在水印中的作用以及水印的理论容量[76]。

2. 视频水印技术

Video 由一系列连续的以及时空域上相关的静态图像组成。因此，通常认为 Video 水印技术与图像中的水印问题比较相似，但事实上图像水印技术和 Video 水印技术有明显的不同。对于图像，可选用的宿主信号空间即像素非常有限；对于 Video，可用信号的空间非常大；视频水印通常强调实时性或者接近于实时，因此对于许多场合，水印算法的复杂性往往会成为一个比较重要的问题。另外一个需要考虑的问题是，Video 实际上是由相关的静态图像序列组成，相对于图像，增加了一些特别的攻击，如帧平均、帧剪裁以及帧交换的可能性。下面简单介绍以下 5 种视频水印技术。

- 压缩域和未压缩域的水印方案：有关在压缩和未压缩的 Video 序列中加入水印的方案的基本原理大部分来自扩频通信的思想，其实现是将一加密的伪随机信号在统计上无感觉地嵌入 Video 中，该视频水印方案主要包括以下 3 部分：①水印信息图像构造，完成对应每帧视频图像的水印信息图像；②水印信息调制后嵌入在视频中；③水印信息提取与检测，完成从视频信息中分离水印信息并进行信息检测，验证水印信息的真伪。相关的文献有 F. Hartung 和 B. Girod 等人在文献[77-79]中提出了未压缩域和压缩域的视频水印；Hsu 和 Wu 提出了对于压缩 Video 的水印[80]，他们将图像的水印方案[81,82]扩展到 Video 序列中，该方案的一个缺点是，对于水印的提取和恢复，需要知道未水印化的 Video 以及水印。Langelaar 等人提出了对于压缩 Video 的两种不同的信息嵌入[83]。Swanson 等人提出在未压缩的 Video 中的多级水印方法[66,84]。
- 基于视频纠错编码的水印方案：Zhao 等人提出的算法是将版权商标嵌入在 Video 的频率域，空间域的亮度信息首先变换到 DCT 的频率域，然后进行量化[85]。算法使用密钥随机地从量化后的系数中选取 3 个系数存储一个版权商标的比特信息，对于嵌入 1 或者 0 ，Zhao 和 Koch 使用高、中、低 3 种尺度定义不同的图案，如果存储一比特的信息需要在块的系数中作显著的改变，就要对这些系数进行处理，形成无效的图案，告诉恢复时在哪个块中没有嵌入信息。类似的文献有 Linnarts 等人提出在 MPEG-2 压缩的 Video 的 GOP 结构编码过程中嵌入信息[86]；Dittmann 等人提出 Video 在水印之前预先解压缩，而在水印后再压缩[87-89]，通过在连续的帧中多次嵌入水印引入冗余，从而在恢复时进行平均。在 MPEG-2 的格式下，视频帧可以 3 种不同的形式进行编码，这类方案中被嵌入的信息的抗解压缩性能需要考虑[90]。
- 基于视频流运动差分矢量的水印方案：在 MPEG 压缩编码算法中，运动预测及补偿技术通常是用于减少帧间的时间冗余度，只有预测到有误差的图像，才被编码。已有文章指出，可以通过微量修改运动矢量中的数据序列隐藏水印信息，这样可使水印的检测非常容易[91]。运用这一思想，该方案[91]从两个方面改进了前一方案[85]：一是将水印嵌入在运动矢量幅值大的宏块中；二是在相角变化小的运动矢

量分量中嵌入水印。在运动向量中嵌入水印,还有另外一种原因,那就是目前的很多视频编码中,如 H.263 系列编码中,通常采用不等长编码(VLC)技术,根据视频中的运动程度而采取不等的保护[92]。水印嵌入在运动的分量中而进行编码,同样有利于对水印的保护;类似的文献还有 Jordan 等人将水印嵌入在对运动补偿预测的动态向量中[93],该方案反映出一种水印如何在视频中嵌入的思想,那就是指向平坦区域的运动向量可以伪随机的方式做轻微修改,所以不会引入任何可视伪像。但有关在运动向量中嵌入水印方案的鲁棒性,需要在实际应用中加以考虑。

- 空间域的视频水印方案:空间域视频水印技术是指在视频信息尚为图像序列时,先在图像原始数据空间中完成水印信息嵌入,再进行视频压缩编码过程的水印设计策略。这类设计策略多来自较为成熟的静止图像的水印技术,按照水印信息嵌入过程,大体可分为两种方案:一种是利用空间域图像特征,直接在空间域完成水印信息嵌入的方案[94,95];另一种则是将视频的原始图像经过一定的变换过程,在变换域中进行水印信息的嵌入,然后经过反变换,再回到空间域的间接嵌入方案[80]。两者相比,第一种更直接,并且通常嵌入算法的硬件实现复杂度较低;而第二种方案可以更充分地利用人眼视觉特性(HVS)完成水印信息的嵌入,如频率特性、小波域特性,使整体算法鲁棒性增强,但实现复杂度也同时加大。
- 其他一些具有特点的方法:Deguillaume 等人提出了将扩频的水印嵌入在 Video 的 DFT 块的系数中[89],这对于几何变换,如放大和位移没有影响。Kalker 等人开发了用于 Video 多播检测应用的水印方法被称作 JAWS(Just Another Watermarking System)[96]。该图案可在几个连续的 Video 帧中重复嵌入,水印检测则使用相关检测。

3. 文本水印技术

文本作为信息传递的重要媒体,其应用甚至超过图像、语音等其他多媒体形式,甚至可以说无处不在。在人们的工作和生活中扮演重要角色的文字信息的传递已越来越多地依赖于电子文档,特别是近年来数字技术的发展、电子出版物和电子图书馆的出现改变了传统的出版和传播观。作为以文字为主的信息表达形式,文本具有其他媒体不同的特点,这些特点决定了基于文本的水印技术和其他的图像、视频等的明显不同。

4. 数字音频水印技术

和图像中的水印技术相似,在音频中嵌入水印,主要是利用语音中的冗余度嵌入水印信息。因为音频对噪声的干扰非常敏感,在音频中加入多余的信息必然会影响原始音质。因此,既要在音频中加入像噪声一样的水印信号,但又不想影响原始的高保真度的音质,这在技术上是一个折中的选择;另外,音频序列可供利用的数据少,因此不可能像图像和视频中那样嵌入太多的水印信息,甚至不能考虑像图像中嵌入多重水印的方案,数字音频水印技术也会是未来版权保护的一个重要方面。

5. 其他类型的水印技术

除上述几种水印技术外,还存在一些其他类型的水印技术,此处不再一一阐述。

5.3 水印的相关研究模型

5.3.1 基于一般通信信道的水印模型

研究水印问题的一种思路是把它看作一种含有隐私的通信系统，由于应用背景不同，可以建立各种形式的水印模型。

1. 基本模型

图 5-2 是一个基于基本通信系统的水印模型。水印的嵌入过程包含两个基本步骤：首先将信息映射为附加模板 W_a，它和载体产品 c_o 的类型一致，而且维数相同。例如，当给图像添加水印时，水印编码器会产生一个二维的像素模板，而给语音添加水印时，水印编码器会产生一个一维的水印信号，这类映射可以用水印密钥实现。接下来把 W_a 加到载体产品 c_o 上，便产生了水印产品 C_W。

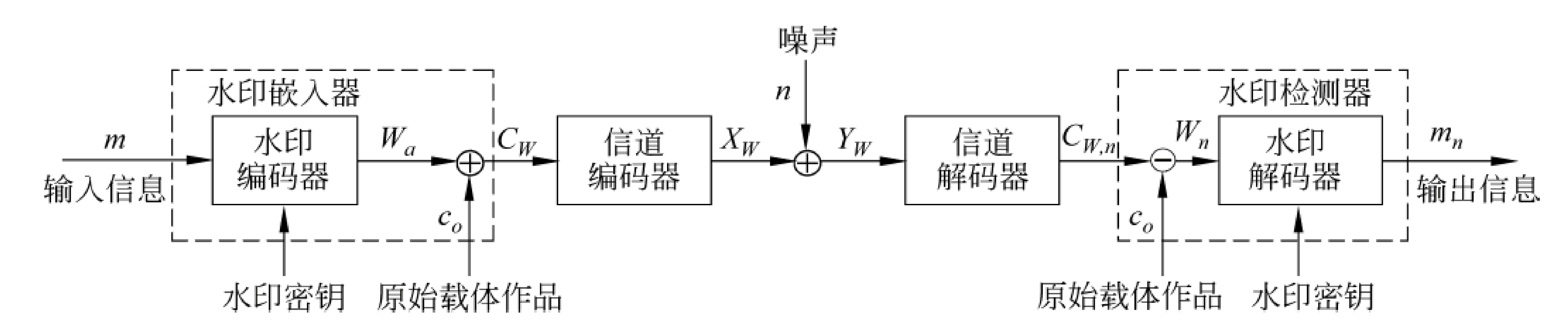


图 5-2　基于基本通信系统的水印模型

2. 依赖于原始载体的水印模型

图 5-3 所示为 W_a 依赖于 c_o 的水印模型。它和图 5-2 所示的模型几乎相同，唯一的区别是，在这个模型中，水印编码器将 c_o 作为另一个输入。这一改变使得编码器可以赋予 C_W 任何值，只要 $W_a = C_W - c_o$。进一步考虑到载体产品是传输信道中噪声过程 $(c_o + n)$ 的一部分，因此这个新模型实际上是发送端携带有附加信息的通信系统。换句话说，新模型中的嵌入器能够有效利用信道噪声，尤其是载体产品 c_o 自身的一些信息。

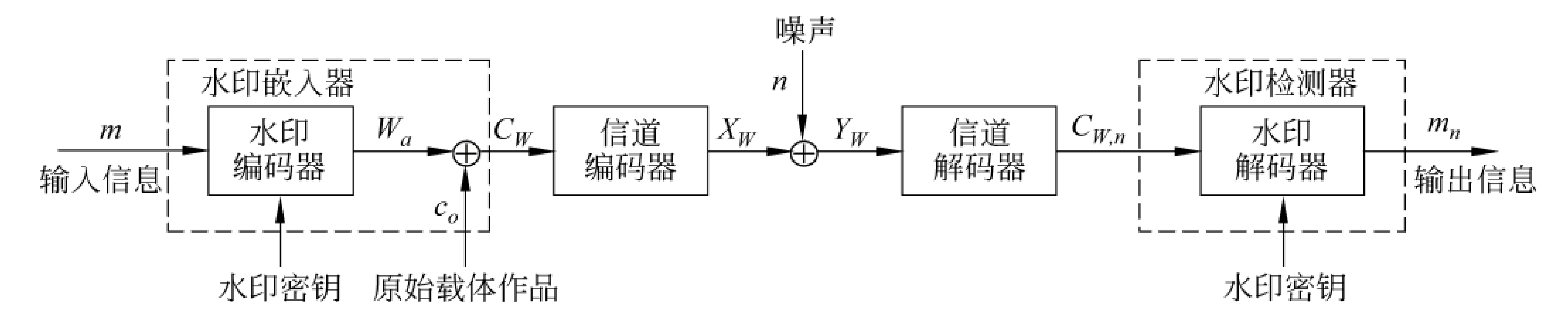


图 5-3　W_a 依赖于 c_o 的水印模型

3. 复用通信的水印模型

两种信息同步通信的水印系统如图 5-4 所示。

在图 5-4 中把载体产品当作和水印信息在同一信号 C_W 中一起传输的另一信息。人

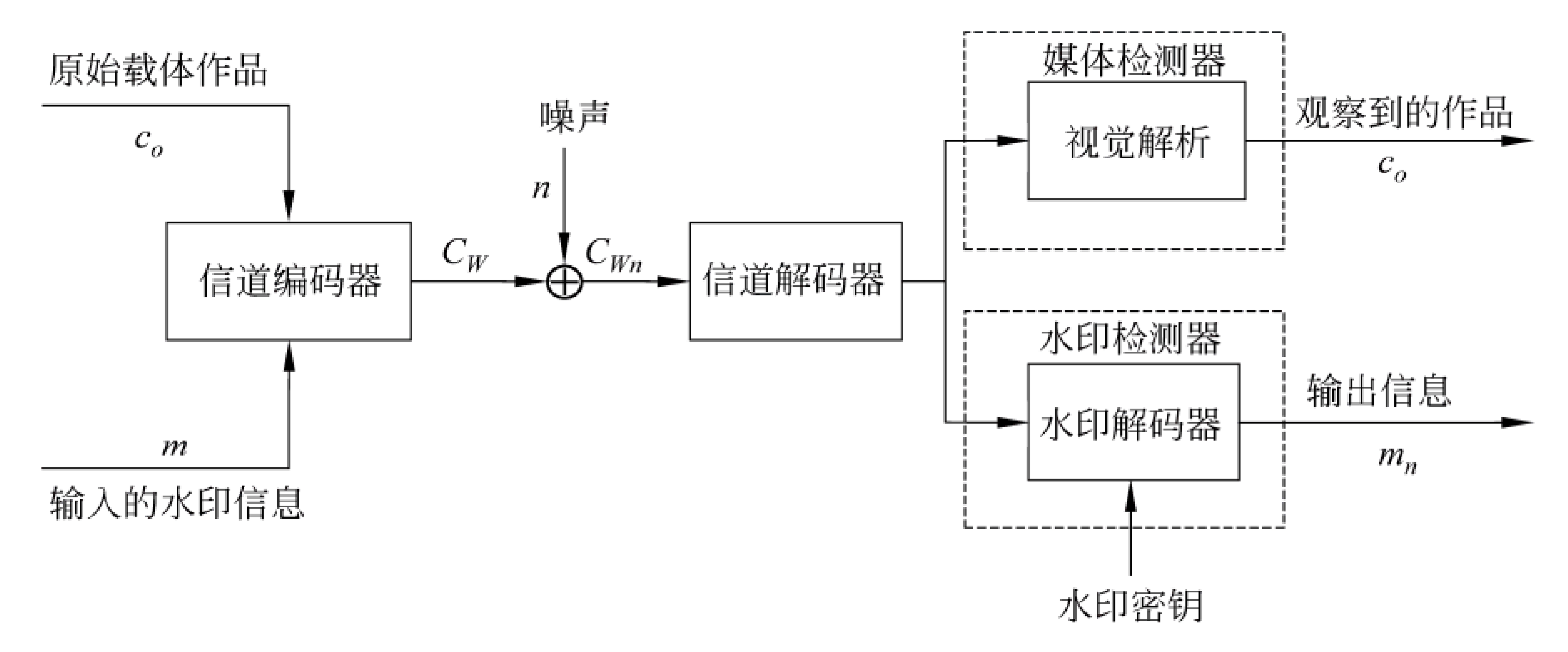


图 5-4 两种信息同步通信的水印系统

和水印检测器这两种完全不同的接收器分别对 c_o 和 m 这两种信息进行检测和解码。信号通过传输信道后同时进入人的感知系统和水印监测器。人在观察 C_{W_n} 时不会受水印的影响，应该观察到和原始载体产品相似的产品。水印监测器在检测 C_{W_n} 时不会受原始载体产品的干扰并得到原始水印信息。

粗略地讲，在以上水印的 3 种模型中，第一种基本模型直接由通信模型映射而来；第二种模型适合于构造基于载体特征的水印方案，像用于版权保护的水印；第三种模型对于构造可视的水印方案是合适的。

5.3.2 水印的子信道分割模型

下面以图像中的水印为对象，探讨子信道水印的含义。Servetto 等人提出了一种水印算法，该算法把一幅图像 X 分成互不重叠的 N 个部分[97,98]。

$$X^{(k)}=[x_1^{(k)},\cdots,x_i^{(k)},\cdots,x_n^{(k)}]\quad k=1,2,\cdots,N;\ i=1,2,\cdots,n \tag{5-1}$$

其中，n 表示每一部分的长度。这些部分可以是 DCT 系数块，也可以是小波子带系数的集合(本书仅将 DCT 系数作为对象进行研究)。同样，将水印信息转换成和 $X^{(k)}$ 一样的形式。

$$W^{(k)}=[w_1^{(k)},\cdots,w_i^{(k)},\cdots,w_n^{(k)}]\quad k=1,2,\cdots,N;\ i=1,2,\cdots,n \tag{5-2}$$

定义一正实向量 $p_i^{(k)}$，表示 $x_i^{(k)}$ 可以容许的最大噪声偏差：

$$P^{(k)}=[p_1^{(k)},p_i^{(k)},\cdots,p_n^{(k)}]\quad k=1,2,\cdots,N;\ i=1,2,\cdots,n \tag{5-3}$$

则加入水印信息的图像可以定义为

$$Y^{(k)}=[x_1^{(k)}+p_1^{(k)}w_1^{(k)},\cdots,x_i^{(k)}+p_i^{(k)}w_i^{(k)},x_n^{(k)}+p_n^{(k)}w_n^{(k)}] \tag{5-4}$$

水印的恢复过程如下

$$\hat{W}^{(k)}=\left[\frac{\hat{x}_1^{(k)}-x_1^{(k)}}{p_1^{(k)}},\cdots,\frac{\hat{x}_i^{(k)}-x_i^{(k)}}{p_i^{(k)}},\cdots,\frac{\hat{x}_n^{(k)}-x_n^{(k)}}{p_n^{(k)}}\right] \tag{5-5}$$

在以上的水印恢复过程中，需要原始的水印 $p_i^{(k)}$ 序列，通常被定义为“私钥水印”系统。另外的方案是在恢复时不需要原始水印序列，通常被定义为“公钥水印”系统。

5.3.3 水印的子信道容量

从广义的角度讲，图像的系数分块之间以及各个分块系数之间都可以看作一种水印

通信的子信道。从以上的讨论中可以看出，如果将图像的特征系数看成通信信道的载体，水印信号看作实际上要传输的信号，那么，在图像中水印最大可能的嵌入容量也就是信道在有噪声的情况下所能容忍的最大噪声容量。假设图像 DCT 系数彼此独立，水印的系数为独立相等分布的随机变量，将图像的系数当作加性噪声，由信息论可以推知：给定信噪方差比，高斯分布噪声具有最大熵值[99,100]，相应的信道容量为

$$C = \frac{1}{2}\log_2\left(1+\frac{\sigma_w^2}{\sigma_x^2}\right) \tag{5-6}$$

但实际的 DCT 系数的分布不满足高斯分布，而是遵循广义的零均值高斯分布

$$f_{GG}(x) = \frac{v\alpha(v)}{2\sigma(1/v)}\exp\left[\left(-\frac{\alpha(v)}{\sigma}\mid x\mid\right)^v\right],\quad \alpha(v) = \sqrt{\frac{\Gamma(3/v)}{\Gamma(1/v)}} \tag{5-7}$$

这里，$\Gamma(\cdot)$ 为伽玛函数，v 与 σ 是正实常数，分别控制概率分布函数的形状和变化。当 $v=1$ 时，广义高斯分布简化为拉普拉斯分布，$v=2$ 时，广义高斯分布简化为高斯分布。有关这方面水印技术的研究，可参见文献[96-98]。

5.3.4　Watson 基于 DCT 的视觉模型

有关在图像中求取最大嵌入容量（最优权值）的问题，一直是构造鲁棒性水印方案的追求。但作为水印的基本特征是无感觉，而且期望能够和原始载体的内容特征相结合地嵌入在载体产品中。这又从另一方面限制了片面强调鲁棒性而忽视人类感觉效果的做法。

感知模型可以基于很多不同的信号表示方式。Watson 模型用到的是块 DCT，也就是把图像划分成不相交的 8×8 像素块。Watson 将模型建立在块 DCT 域上是为了将其应用于 JPEG 图像压缩的原理是将图像转换到块 DCT 域，并根据频率确定步长对所得项进行量化。Watson 模型由一个敏感函数、两个基于亮度和对比度掩蔽部分以及一个合并部分组成[101]。

- 敏感度：该模型定义了一个频率敏感度表，表中的每个元素 $t[i,j]$ 表示每块中在不存在任何掩蔽噪声的情况下，可被觉察的 DCT 系数的最小幅度，也就是产生一个单位 JND（刚好能察觉的差别）的系数变化值，所以这个值越小，说明人眼对该频率越敏感。
- 亮度掩蔽：亮度自适应是指，如果 8×8 像素块的平均亮度较大，那么 DCT 系数被较大的数值修改也不会被察觉。为了解决这个问题，Watson 模型对每一像素块 k，根据其 DCT 项对敏感度表中的 $t[i,j]$ 进行调整。亮度掩蔽阈值
$$t_L[i,j,k] = t[i,j]\,(c_o[0,0,k]/c_{o,o})^{\alpha_T} \tag{5-8}$$
式中，α_T 为一常数，通常取值为 0.649，$c_o[0,0,k]$ 为原图像中第 k 块的 DCT 系数，$c_{o,o}$ 为原图像中 DC 系数的平均值。$c_{o,o}$ 也可以设定为一个代表图像预期强度的常数。从式(5-8)可以看出，在一幅图像中，比较明亮的区域可以在不被察觉的情况下进行较大的改动。
- 对比度掩蔽：亮度掩蔽阈值 $t_L[i,j,k]$ 的取值要受到对比度掩蔽的影响。对比度掩蔽阈值 $s[i,j,k]$ 的计算表达式为

$$s[i,j,k] = \max\{t_L[i,j,k], \mid c_o[i,j,k] \mid^{w[i,j]} t_L[i,j,k]^{1-w[i,j]}\} \tag{5-9}$$

式中，$w[i,j]$ 是一个 0～1 的常数，而且会因频率系数的不同而不同。在 Watson 模型中，所有 i、j 的 $w[i,j]$ 都被取为 0.7。最终阈值 $s[i,j,k]$ 估计的是块 DCT 的各项在一个 JND 范围内可进行的变化，这些阈值称为间隙。

- 合并：在对原图像 c_o 和失真图像 C_W 进行比较时，首先要计算对应的 DCT 系数的差值 $e[i,j,k]=C_W[i,j,k]-c_o[i,j,k]$，然后将这些差值除以各自的间隙 $s[i,j,k]$，得到每一项的可感知距离 $d[i,j,k]$，即

$$d[i,j,k] = \frac{e[i,j,k]}{s[i,j,k]} \tag{5-10}$$

式中，$d[i,j,k]$ 是用 JND 倍数或分数表示的第 k 块中第 (i,j) 个频率的误差。

5.4 水印系统的一般性构架

从信号处理的角度看，对多媒体产品的水印化可当作是将一种信号(水印信息)加入另一种信号(宿主多媒体)的一个过程。通常可用一数字信号 W 表示实际的水印信号：

$$W = \{w(k) \mid w(k) \in U, k \in \hat{W}^d\} \tag{5-11}$$

其中，$\hat{W}^d$ 表示维数 d 的水印领域，$d=1,2,3$ 分别表示音频、静止图像和视频水印，称 W 为“原始水印”，U 表示水印信号的值域，可以是二进制的值 ($U=\{0,1\}$ 或者极性符号 $U=\{-1,1\}$)[102,103]或者高斯噪声[94,104]。在文献[104]中，Voyatzis. G 等人定义了水印系统的一般性构架(GWF)模型，而且将水印的基本构架用 6 个元素的一个组合 (X,W,K,G,E,D) 表示。这个模型可以分成 3 个部分：水印创建、水印嵌入和水印检测，如图 5-5 所示。

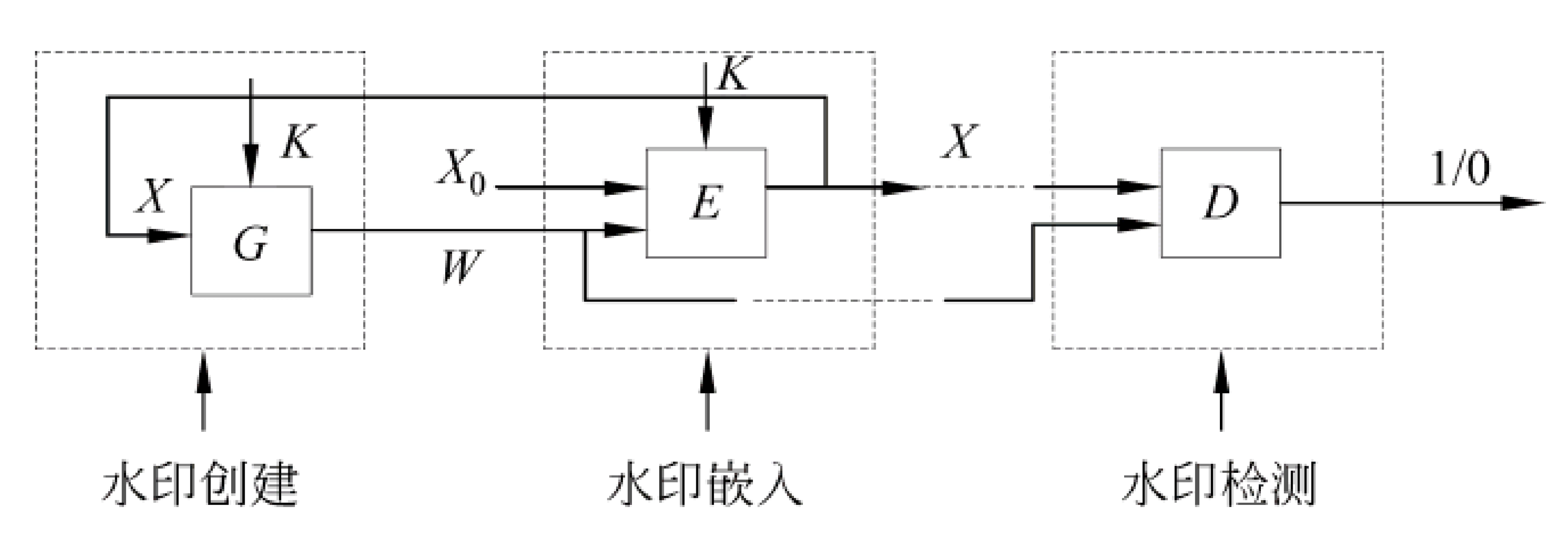


图 5-5　GWF 模型

X 表示所要保护的数字产品 X 的集合。

W 表示所有可能的水印信号的集合。

K 是 ID 数的集合(即整数参数的集合)，也称作水印的密钥。

G 表示利用密钥 K 和待嵌入水印的数字产品 X 共同生成水印的算法

$$G: X \times K \to W \quad W = G(X,K) \tag{5-12}$$

E 表示将水印 W 嵌入数字产品 X_0 的水印嵌入算法

$$E: X \times W \times K \to X \quad X_W = E(X_0, W, K) \tag{5-13}$$

其中，X_W 表示嵌入水印后得到的数字产品。

D 表示水印检测算法

$$D: X \times K \rightarrow \{0,1\} \tag{5-14}$$

其中，$D(X,W)=\begin{cases}1, & W \in W\ (H_1)\\ 0, & W \notin W\ (H_0)\end{cases}$，$H_1$ 和 H_0 表示二值假设检验，分别表示水印存在和不存在。

5.5 水印的基本特征和应满足的必要条件

为了形成对于版权保护的可信赖的基础或者对于数字产品的内容认证，水印应满足一些基本要求。

- 不可感知性：水印嵌入不能产生可感知的数据变化，即加水印的产品 X_w 与原始产品 X_0 具有感知相似性，可表示为 $X_w \sim X_0$。
- 密钥唯一性：不同的密钥应产生不等价的水印，即对任意产品 $X \in \boldsymbol{X}$ 和 $W_i = G(X, K_i)$，$i=1,2$，满足 $K_1 \neq K_2 \Rightarrow \boldsymbol{W}_1 \not\approx \boldsymbol{W}_2$。
- 水印有效性：水印方案中只采用有效的水印。对于特定的产品 $X \in \boldsymbol{X}$，当且仅当存在 $K \in \boldsymbol{K}$，使得 $G(X, K) = W$，则称水印 W 是有效的。
- 不可逆性：函数 $W = G(X, K)$ 是不可逆的，即密钥 K 不能由函数 G 或水印 W 逆推出来。不可逆性意味着对任何水印信号 W，不可能找到另一个有效水印与 W 等价。
- 产品依赖性：函数 G 利用相同的密钥和不同的产品作为参数时，应该产生不同的水印信号。即对任意密钥 $K \in \boldsymbol{K}$ 和任意产品 $X_1, X_2 \in \boldsymbol{X}$，均满足 $X_1 \not\sim X_2 \Rightarrow W_1 \not\approx W_2$。
- 多重水印：通常，一个数字产品可以用其他密钥多次嵌入水印。这一特性有利于众多分销商嵌入不同的标记，也会被盗版者或侵权者利用。当 $X_i = E(X_{i-1}, W_i)$ 时，对任意 $i \leqslant n$，必须满足 $D(X_i, W_i)=1$，其中 n 必须满足 $X_n \sim X_0$ 且 $X_{n+1} \not\sim X_i$。
- 可靠性检验：肯定检测输出有一个可接受的最小精度。用 P_{fa} 表示虚警概率，应该满足：

$$p_{fa} < p_{thres} \tag{5-15}$$

  其中 P_{thres} 是合适的概率阈值。
- 鲁棒性：令 X_0 是原始的产品，而 X_w 是其水印版本，满足 $D(X_w, W)=1$。记 $Y = M(X_w)$ 及 $Y' = M(X_0)$，其中函数 M 表示对数字产品的多媒体数据处理操作，则应该满足：$D(Y, W)=1$，$\forall Y \sim X_w$ 且 $D(Y', W)=0$。
- 计算效率：水印算法应能用软硬件有效地实现，水印嵌入和检测算法应足够快，以满足对分布式网络上的多媒体数据进行监控和管理的要求。

5.6 对水印的攻击

在开放式网络数字产品的分发过程中，盗版者可能会对版权化的产品进行中间搭线攻击，如图 5-6 所示。一般包括以下 3 种可能的情况。

- 非法进入：盗版者企图随意删除水印版权信息，在没有允许的情况下从网站上接收数字产品。
- 蓄意篡改：盗版者出于恶意对数字产品进行修改，通过提取/插入特征对产品进行重发，原始产品则丧失了可认证性。
- 损害版权：盗版者接收到数字产品，在没有获得版权者许可或者授权的情况下进行产品重新销售。

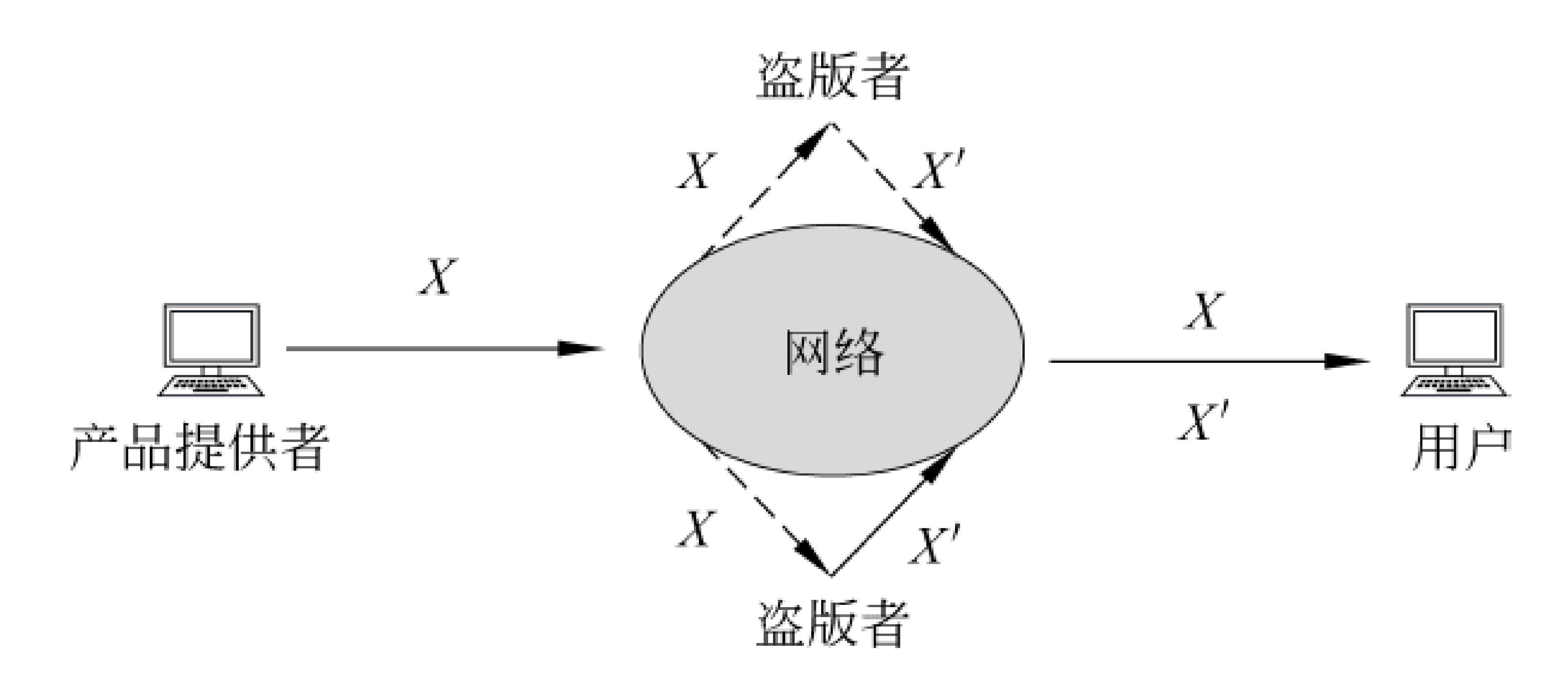


图 5-6 水印遭攻击模型

下面列举了一些常见的信号处理操作和攻击方法。

(1) 有损压缩：这是一类最常见的处理，在图像认证中甚至被看作是可接受的失真处理。常见的有损压缩如 JPEG、JPEG-2000、H. 261、H. 263、MPEG-2、MPEG-4 MPEG-2 audio、MPEG-4 audio、G. 723 等。

(2) 加性与乘性噪声：如高斯白噪声、均匀噪声、斑点噪声、椒盐噪声等。

(3) 低通滤波：包括线性和非线性滤波器。常用的有中值滤波、同态滤波、高斯滤波、均值滤波等。

(4) 增强处理：如锐化、钝化、直方图均衡、Gamma 校正、图像恢复等。

(5) 几何失真：包括局部或全部的几何变换，如平移、旋转、缩放、裁剪、图像翻转、行或列删除、尺度变换。

(6) 统计平均和共谋攻击(Collusion Attack)：利用同一幅图像的多个副本，每个副本嵌入了不同的水印，可以通过对这些图像进行平均或利用每副图像的一小部分重新组合新图像去除水印。

(7) Oracle 攻击：利用公开了的水印解码器，对加水印图像作微小修改并反复进行，直到水印解码器无法检测到水印为止。

(8) 多重水印攻击。

在实际应用中，多媒体的失真往往是由多种处理方法产生的综合失真。著名的 StirMark[106] 测试软件可以提供一系列的图像处理操作，StirMark 还提供了一个水印系统测

试方案，用于比较、评估各种水印方案。

5.7　水印的性能指标评估

本节列举一些在本文中将涉及的几项常用的水印测试指标[107]。对于一个具体的应用，这些指标（或者其中的部分）将能够对设计算法以及水印化的效果从不同的侧面给予定性的参考。

（1）无感觉性(Imperceptible)：这是对水印算法的最基本的要求。嵌入在多媒体中的水印信号不能过分明显，让人稍加注意，就能够将宿主信号和水印信号部分地或者全部分辨出来。

（2）峰值信噪比(Signal-to-Noise Ratio)：主要是针对无感觉性的一个具体测试指标，它反映了水印作为“噪声”加入在图像上对宿主图像整体改变的一个程度，通常用来衡量水印的不可视性以及数据隐藏的效果。

$$PSNR = 10\log_{10}\left(MN\max_{m,n} I_{m,n}^2 \Big/ \sum_{m,n}(I_{m,n}-\hat{I}_{m,n})^2\right) \tag{5-16}$$

单位为 dB，$I_{m,n}$、$\hat{I}_{m,n}$ 分别表示原始的和水印化的图像像素，M、N 分别表示图像的行和列的大小。

（3）相关系数(Correlation Coefficient)：用来测量嵌入的和提取水印之间的相似性。归一化的相关系数如下。

$$\rho(w,\hat{w}) = \frac{\sum_{i=1}^{N_w} w(i)\,\hat{w}(i)}{\sqrt{\sum_{i=1}^{N_w} w^2(i)}\,\sqrt{\sum_{i=1}^{N_w} \hat{w}^2(i)}} \tag{5-17}$$

这里，$w(i)$、$\hat{w}(i)$ 分别表示嵌入的和提取的水印信号，N_w 是水印的长度。

（4）归一化的汉明距离(Normalized Hamming Distance)：如果水印由二进制的元素组成，汉明距离则反映了两个相似的嵌入水印序列和提取水印序列之间的差别的程度。

$$p_{HD}(w,\hat{w}) = \frac{1}{N_w}\sum_{i=1}^{N_w} w(i) \oplus \hat{w}(i) \tag{5-18}$$

这里，w、$\hat{w}$ 以及 N_w 和式(3-20)中的定义一样，$\oplus$ 表示异或操作。

（5）计算的复杂性：依赖于特殊的应用以及水印化的多媒体，计算复杂性是衡量水印算法可行性的一个重要因素。例如，在 DVD 播放器中，水印的提取有可能要求具有实时性，因此设计的算法要在保证安全的情况下尽量简单。对于静态图像的水印，为了高的、安全的、知识产权的永久保护，设计的水印算法应尽可能鲁棒和复杂，这不受实时性的影响。因此，对计算复杂性的要求会随着应用的变化而变化。

第 6 章 水印在数字多媒体产品保护中的应用

随着数字网络技术的完善和发展，散布在网络上的多媒体数字产品的版权问题受到了高度的重视。作为数字产权保护的应用技术之一，零知识证明、公钥数字水印的基本思想是将密码学中的公钥加/解密的概念引入到水印的认证方案中。本章就是基于密码学的一些协议思想构造了数字产品的版权证明协议。

6.1 数字产品的网络分发模型

版权所有者用自己的私钥在多媒体数字产品中嵌入版权信息，然后将水印化的产品在公开的网络上发布，如图 6-1 所示。在使用公钥水印[108-111]的情况下，任何人都可以用公开的算法对水印进行提取、认证，安全的协议要保证即使在诸如 Internet 这样的普通安全性的环境下，仍能达到水印的可靠认证。

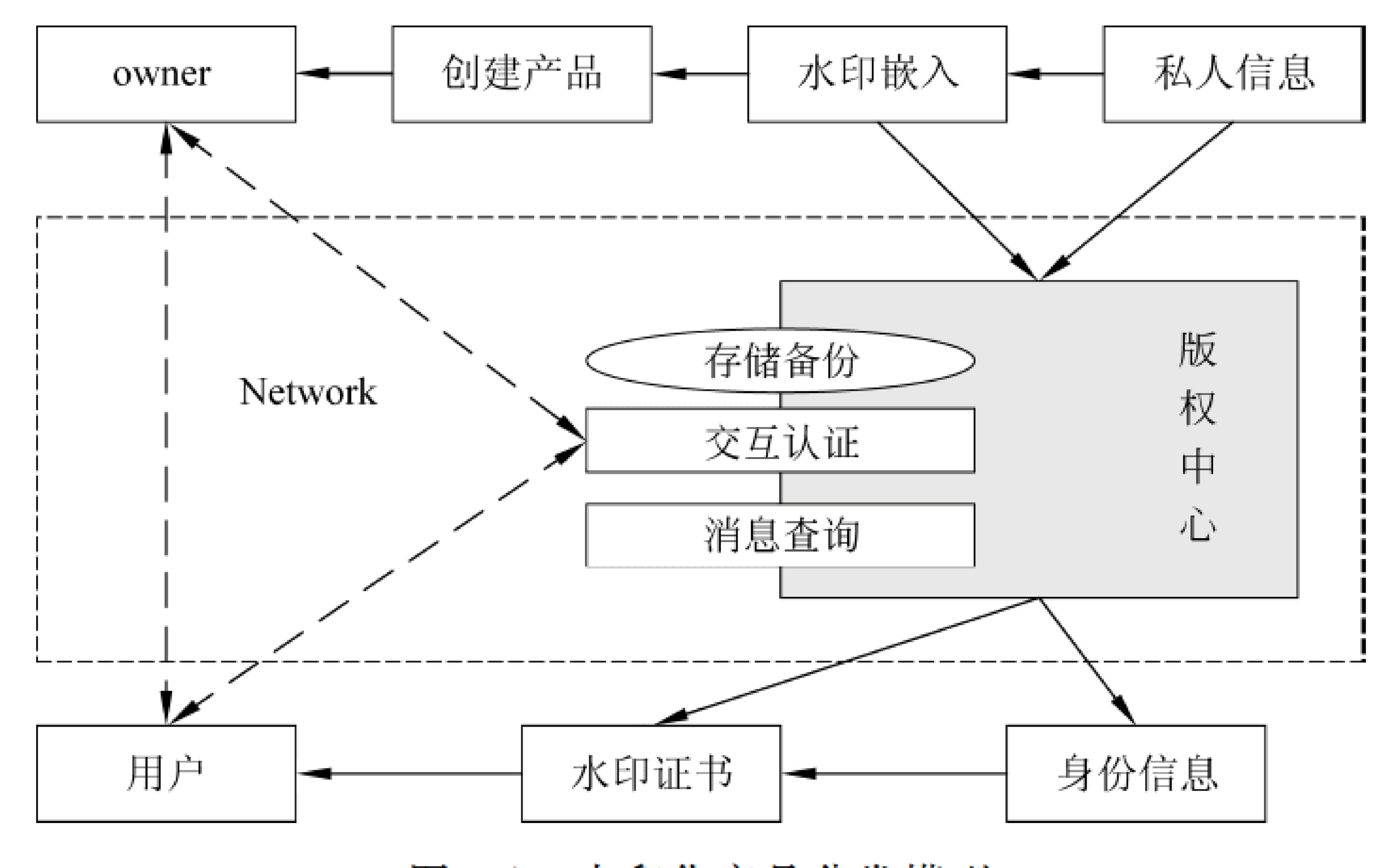


图 6-1　水印化产品分发模型

6.2 水印的创建和认证

认证模型中包括一个安全的密钥分发中心(KDC)；一个可信赖的版权管理机构(TCM)；产品的使用用户(User)或者购买者；版权所有者(Owner)或者也可以是被授权的

产品的提供者、代理商等。

- KDC 负责所有相关密钥的产生、管理和分发。每个参与者都可以向 KDC 申请产生自己永久的或临时的会话密钥对。这里，假设密钥可以根据各种要求安全地产生和分发。
- TCM 为可信的版权管理机构。TCM 在自己的服务器上能够对系统内用户的产品进行注册、鉴别、认证、跟踪、管理等。在水印版权认证系统中扮演可信的第三方而参与执行协议。对所有参与者，假设 TCM 不泄露有关各方的任何私人的秘密信息。当发现有非法的"假冒伪劣"产品或者有欺骗发生时，它可以终止执行交互认证协议、公告产品违法等。同时，TCM 还是最终版权的终裁者。
- Owner 是产品的版权所有者/提供者，Owner 在自己的 Web 站点提供自己的多媒体数字产品。在这些产品中，Owner 通过加入自己的秘密水印而实现版权的保护，当发现自己的版权被盗时，可向 TCM 申请进行版权的认证和追踪，同时，Owner 在 TCM 的管理范围中应能够对自己的水印版权进行正确的提取和证明。
- User 是多媒体产品的使用用户，购买产品时，User 可要求 Owner 出示证明表明交易的产品是经过注册的合法的产品。同时，User 有权利向 TCM 申请对所购买的数字产品进行版权鉴定。对于 TCM，User 和 Owner 享受的权力待遇应该一样。

基于以上要求，在 Owner、User 和 TCM 之间组成了一个简单的三方版权认证系统，如图 6-2 所示。

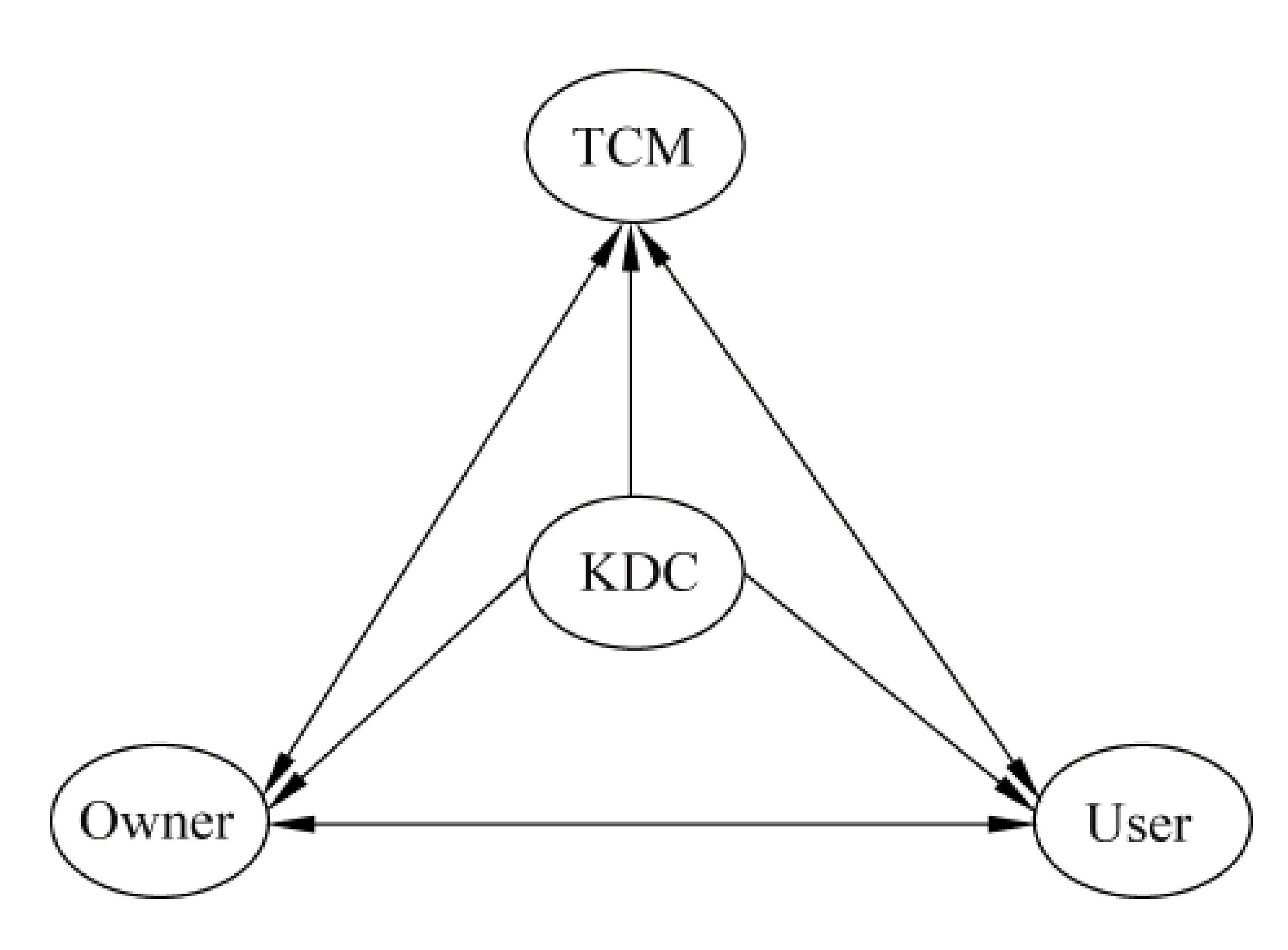


图 6-2　基于三方认证框图

6.3　水印版权的认证方案

版权的认证方案包含 4 方面内容：版权认证系统的初始化、创建者版权的注册、证明以及显示。

(1) 初始化过程包括建立一个 KDC 以及 TCM。在初步的协议中，首先假定 KDC 和 TCM 是安全和值得信赖的，Owner 是真正的多媒体产品的创建者，不会在交易过程中进行欺骗，User 是诚实的多媒体产品的使用用户。

(2) 注册在 Owner 和 TCM 之间进行，Owner 向 TCM 发出注册申请，TCM 在自己的服务器中输入 Owner 的注册身份 Id 和数字产品 x_0，经过一番搜索之后(这里的搜索主要指对输入的 Id 及 x_0 必须执行两个子程序，即相似性检验 $sim(\cdot)$和相关性检验 $relat(\cdot)$程序)，当得知服务器的存储档案中至今还没有注册过相同的甚至是极其类似的产品，则将 Id 及 x_0 输入构造的 hash 函数，输出一与 Owner 的 Id 及 x_0 相关的代表 TCM 签名的确认号 Id_{TCM}，将 Id、x_0、Id_{TCM}及相关内容在存储器上建立新的档案，注册成功！TCM 将以上结果用证书的形式连同注册时间发向 Owner。该过程描述如下。

Owner：$\{Id, x_0\} \rightarrow$ TCM
TCM：$sim(Id, x_0) =$ no ?
$relat(Id, x_0) =$ no ?
$W = regist(Id, x_0, t)$
$W \rightarrow$ Owner

(3) 产权的认证涉及 User。User 得到数字产品后，想知道自己买来的东西是否是注册过的正版产品，最好的办法是向 TCM 求助，以便得到版权的认证，TCM 验证由它先前签发的 Id_{TCM}，以及发证书的时间 T，执行一验证程序 $ver(Id_{TCM}, T)$，如果产品通不过，此程序则被否定。如果通过，TCM 则面临是否注册过以及注册过的是正版，还是蒙混过关的赝品？TCM 执行 $sim(\cdot)$和 $relat(\cdot)$程序，由 $prov(\cdot)$的结果断定产品是否正版。在这一过程中，$sim(\cdot)$和 $relat(\cdot)$程序的结果必须同时得到满足。描述过程如下。

User：$x_w \rightarrow$ TCM
TCM：$ver(Id_{TCM}, T) =$ true ?
$sim(x_w) =$ ok?
$relat(x_w) =$ ok?
$prov(Id_{TCM}, x_w) =$ ok?

(4) 在步骤(3)中，TCM 只能向 User 肯定发送来的数字产品已经进行了产权注册，但它并不能告诉 User 原始产品的提供者是否在产品中嵌入了水印以及用什么方式或者将什么水印信息嵌入其中($x_w \neq x_o$)。因此，TCM 可要求 Owner 进一步协助证明 x_w 的确是 Owner 自己水印化的产品。由 Owner 提供水印的嵌入公钥 k_p，TCM 根据嵌入算法 $emb(\cdot)$计算：

Owner：$\{Id_{Owner}, k_p, k_{emb}\} \rightarrow$ TCM
TCM：$hash(Id_{Owner}, k_p) \rightarrow W$
$emb(x_o, W, k_{emb}) == x_w$
$(x'_w = x_w) ==$ true!

(5) 进一步，如果有版权纠纷问题，作为真正的版权拥有者，只有 Owner 才能提供正确的水印，但有时有多个 Owner 同时声明对产品拥有所有权，这就引起了产权纠纷问题，在很多密码学中，解决这类问题的一种方法是验证签名的时标，但在水印版权方面，这种方法需要进一步研究。例如，同样是信息的嵌入，为什么攻击者不可以变动自己的时标信

息？不过，我们的方案还是将版权的注册和取得的证书、执行的时间相连。这样，即使攻击者能够在嵌入信息中篡改时标，但它能否经过认证，则需要有关的证据支持。

Owner：$algorithm(x_w, k_{extract}) \to W', x_0'$
$prov\ (W'=W)==$ yes !
$prov\ (x_0'=x_0)==$ yes !
$hash^{-1}(Id_{TCM}, k_S, t) = Id_{Owner}$

(6) 如果发生所谓的版权纠纷，最终的解释就需要真正的政府法律机构的仲裁。

6.4 数字水印的认证协议

6.4.1 相关认证协议

1. TCM 的初始化协议

基于 Schnorr 身份识别方案[112]，在 TCM 建立初始化的协议，该协议主要涉及对产品版权的正常注册以及认证的初始化过程，具体如下。

1. 令 p 是一个大素数，使得 $Z_P{}^{\#}$ 的离散对数问题是最难解的。 2. q 是一个 $p-1$ 的大的素因子。 3. $\alpha \in Z_P{}^{\#}$ 有阶 q（这样，一个 α 能从本原元的 $(p-1)/q$ 次幂中计算出）。 4. TCM 还建立一个安全参数 r，满足 $q \geqslant 2^r$。 5. TCM 规定一个安全的水印注册方案，该方案具有一个秘密的注册算法 $regist(\cdot)$ 和一个公开的验证算法 $ver(\cdot)$。 6. TCM 规定一个安全的散列函数 $hash(\cdot)$，所有信息在注册前要进行散列。 7. 参数 p、q、α 以及验证算法 $ver(\cdot)$ 和函数 $hash(\cdot)$ 全部公开。 r 是一个安全参数，如果随机选择 r，冒充者就会猜测出正确的 r 值的概率为 2^{-r}，r 值的选择取决于系统的安全要求。

2. 产品的注册

注册在 TCM 和 Owner 之间进行，Owner 将自己的版权信息进行加密，并且将加密结果发向 TCM，TCM 对来自 Owner 的申请进行注册，然后将注册证书发向 Owner。Owner 将发来的注册过的证书当作原始的水印信息经过 $hash(\cdot)$ 函数计算后将结果嵌入自己的多媒体产品中。

1. Owner 秘密地选择一个随机指数 a，$0 \leqslant a \leqslant q-1$，并计算 $v = \alpha^{-a} \bmod p$，且把 v 给 TCM。 2. TCM 产生一个注册证书：$Id_{TCM} = regist(Id_{Owner}, v)$ 3. TCM 将证书 Id_{TCM} 发向 Owner。 4. Owner 通过一哈希函数得到相关的嵌入在多媒体中的水印 $W = hash(x_0, Id, k_s, t)$。

3. 水印信息的显示及证明

该协议在 Owner 和 User 之间进行。作为正常的用户，User 有理由在购买产品时，向 Owner 提出要求出示合法的版权证明她/他出售的产品的合法身份，因此，在二者之间形成一个秘密版权的证明交换协议。当然，这个过程可以在 TCM 的参与下进行，也可以在 TCM 不参与的情况下而有事先的授权，如果有必要，User 可以将 Owner 发向她/他的信息发向 TCM 进行进一步的原始认证，Owner 也可以向 TCM 要求对 Owner 的合法性进行评估。

1. Owner 选择一个随机数 l，$0 \leqslant l \leqslant q-1$，并计算 $\gamma = \alpha^{l} \bmod p$。
2. Owner 发送 $\{Id_{Owner}, s\}$ 和 γ 给 User。
3. Owner 通过检查 $ver(Id_{TCM}, v, s)$ =true 验证 TCM 的签名。
4. User 选择一个随机数 r，$1 \leqslant r \leqslant 2^{t}$ 且把它送给 Owner。
5. Owner 计算：$y = (l + ar) \bmod q$ 且把 y 送给 User。
6. User 验证 $\gamma = \alpha^{y} v^{r} \pmod p$。

6.4.2 协议的安全性分析

基于 Schnorr 身份认证方案的安全性建立在计算离散对数的难题上，作为密码学上的身份认证协议，它是可靠和完备的，将其用于公开网上水印的版权认证系统中，避免了在使用私钥水印系统中必须传递密钥或使用原始数据才能进行水印检测和认证的缺点。

(1) 模仿攻击：就像上面协议提到的，在安全参数 r 确定的情况下，如果 Owner 随机地选择 t，冒充 Owner 欺骗 User 的成功概率就为 2^{-t}。实际使用中，协议的每一次迭代都规定在一多项式时间内完成。这样，根据具体的计算效率，t 的选择不一定需要很大。

(2) 水印算法及验证算法是公开的，但是算法每次迭代的某些临时参数不同，这样可保证信息交换的新鲜性，而防止在交互认证中出现重复性的攻击现象，协议中的算法理论上都是不可逆的。

(3) 阻止合法产品被非法重新分发：如果偷窃者能够以“合法”的身份伪造 Owner 的产品在网络上出于私有利益进行重发销售，Owner 可向 TCM，甚至向法庭提出诉讼，在公证机构的监视下，Owner 用嵌入密钥揭示出自己注册的原始水印（合法的 Id 或者商标），从而证明她/他是原始产品的版权拥有者。

(4) 在整个结构中，我们始终认为 TCM 是诚实和可靠的，如果 TCM 不可信，甚至 TCM 还有可能和其他用户以及创建者的一方共谋欺骗另一方。同样的不可信赖性也可能发生在 KDC 的管理上。对于这些问题，本书没有进行深入讨论，文献[112]有所提及。王彩纷教授在其博士论文“有关密码学中的基于不可信和半可信的总裁机构的协议的安全性研究”中对这一问题进行了详细讨论[113]。

(5) 整个认证协议对网络的安全性要求较低。

6.4.3 公钥水印产权的检测和跟踪

(1) 作为公钥水印在产品中的嵌入，任何合法的消费者或机构都可以通过公开的验

证算法对数字产品的版权加以认证，这在一定程度上能够抑制网络上无注册的非法产品的传播；另一方面，也能保证消费者个人应有的合法权利和利益。

(2) 交互式认证协议使得盗版者对原始的水印化产品的重发或者“倒卖”变得困难。因为购买者可通过版权管理机构的“帮助”认证销售者的版权以及合法注册身份，如果二者不符，则交易被终止。从这一点上讲，尽管交互式认证协议似乎和水印本身的技术没有非常紧密的关系，但作为水印的实际应用，则是不可缺少的，也是水印技术的一个重要部分。

(3) 对原始水印化产品的修改或改变，则通过对产品中嵌入“证书”信息的检测得到估计，产品在某个中间环节被修改，有可能被比较明显地显示出来，或者尽管没有明显的修改痕迹，但嵌入其中的版权数据有一定的变化(脆弱水印)，这一点可能更符合对脆弱水印特征的定义。作为 TCM 的服务器可以对这种修改进行检测、估计，针对不同的情况进行处理。

(4) 基于公钥水印的认证，避免了在信道上传递大量的有关原始产品的数据(私钥水印)，对于信道上的偷听者，想获得对产品中水印的攻击所需的信息是困难的，或者说她/他可能需要付出更大的代价。这样，在公开网上有利于对数字版权的保护。

6.5 基于零知识证明的水印认证协议

为了阻止对产品中版权的攻击，版权所有者不期望在公开的版权认证过程中泄露太多的原始水印(版权)信息，而且有必要将它视为只有自己知道的秘密。但作为数字产品要公开的销售，他又不得不向其他人揭露足够的信息，使别人相信产品是他自己创作的，或者说，他具有产品独一无二的知识产权。另一方面，购买者在购买产品时，也可能对产品的合法性进行怀疑，希望能够揭示足够的信息证明产品来自合法的作者或者合法的软件公司。

零知识证明的本质是人们可以证明一个事实的知识，而对其他人不泄露该知识的一种方法[112]。零知识证明协议的特性可以很好地应用于水印的认证系统，以解决上述数字版权认证中的问题。

6.5.1 基于离散对数的零知识证明协议

选择公开的大素数 p 和生成元 q ，以 q 为基进行 mod p 计算：$M = q^x (\bmod\ p)$ ，公布 M 而保持 x 为秘密，显然，给定 M 确定 x 非常难。Owner 通过证明 x 的知识确认自己的身份。

(1) Owner 产生随机数 y，计算 $N = q^y (\bmod\ p)$，将 N 发向 User。

(2) User 知道 M 和 N，依赖于投硬币的结果要求 Owner

要么给出 y，验证 $N = q^y (\bmod\ p)$ 。

要么给出 $y+x(\bmod(p-1))$，验证 $MN = q^{y+X(\bmod(p-q))}$。

(3) Owner 完成以上步骤之一。

(4) 数据 y、N 被丢弃。在协议的每次迭代中，都产生新的数。

在上面的协议中，Owner 每次欺骗 User 的概率为 1/2。对协议迭代 n 次，欺骗的概率就为 $1/2^{-n}$。实际中，协议的执行可能要求在一定时间内完成，因此 n 的值不一定很大。

6.5.2 零知识证明协议在水印认证中的应用

以上协议中，如果 Owner 不知道有关 x 的知识，就无法满足(2)中的后一个要求，在证明自己的确知道 x 时，使用了“秘密隐蔽”特性。协议中，将对 M 对数的计算问题转化为对 MN 的证明，其目的是通过证明相关的一个问题使另外的人知道原始问题的答案。另一个要说明的是，该协议是问答式认证协议，需要通过“隐蔽”完成。问答式协议保证诚实的一方证明者被要求揭示足够的信息限制欺骗的概率。在隐蔽的情况下，证明者要么解决转换的问题，要么证明对事实的隐蔽是完全清楚的，即转换的问题是从原始问题中推导而来[114]。零知识证明协议也可以构造成非交互式的形式，也就是将所有需要多次提问的问题一次性回答完毕。

零知识证明协议的特性决定了它在公钥水印认证中的应用[114,115,116]，文献[112]中给出了基于图同构的零知识证明构成的图像签名系统，这里假设 Owner 在一个 Web 站点具有在认证中使用的一些数据，但最终这些数据都要被嵌入要提供的多媒体中作为 Owner 版权的声明。如果这些嵌入的数据信息在认证过程中被知道，那么攻击者就可以充分利用这一点，如假扮 Owner 而非法地重新销售 Owner 的多媒体产品等。另一方面，对于诚实的购买者，Owner 要能够揭示自己嵌入的版权信息证明自己是产品的合法版权所有者。因此，需要 Owner 嵌入的版权信息既能公开被认证，同时又保留原始的版权信息使用零知识证明协议对水印信息的认证，能使嵌入的版权信息充分被其他人证明，但本身足够隐密。想获取有关它的信息非常困难。

6.5.3 零知识证明协议下水印的创建

Owner 首先将自己的数字产品 I 和身份信息 Id_{Owner} 向 TCM 注册，TCM 经过一番检验后，认定 I 和 Id_{Owner} 属于合法，则产生一相关的由 TCM 签名的鉴定信息。这里假设 TCM 的信息可被表示成模 p 上的一个整数 A，TCM 将自己的鉴定信息用证书 Id_{TCM} 的形式连同注册时标发向 Owner，即

$$\text{Owner}: \{I, Id_{Owner}\} \rightarrow \text{TCM}$$

$$\text{TCM}: Id_{TCM} = Sign_{TCM}\{I, Id_{Owner}\}$$

$$\{Id_{TCM}, T\} \rightarrow \text{Owner}$$

(1) Owner 在获得的证书中得到 A，A 将作为版权的水印嵌入原始产品 x 中，同时 A 也可表示成一长度为 N，mod p 上的二进制序列 A。定义：

$$A = \{a, 0 \leqslant i < N\} \quad a_i \in \{0,1\}$$

(2) Owner 选择素数 p、q，用基 q，mod p 的离散对数对嵌入的信息进行计算，即

$$m = q^A (\bmod p)$$

公开 m 以及保持 A 为秘密。

(3) Owner 同时产生另外的 $t-1$ 个小于 $p-1$ 的随机数 $B_i(1\leqslant i\leqslant t-1)$，分别计算

$$m_i = q^{B_i} (\bmod\ p-1)$$

表面上看，这 $t-1$ 个 m_i 与 m 没有任何差异，似乎都是等长为 N 的二进制序列。m 和 m_i 共组成了 t 个元素的集合 $w=\{m_1, m_2, \cdots, m_{t-1}, m\}$。将 w 中的元素 m_i 以及 m 的先后顺序随机地置乱，然后串接起来，可形成长度为 $N\times t$ 的二进制比特串，仍记为 w'。

(4) Owner 用序列 w' 乘以系数 $\alpha_i(\alpha_i\geqslant 0)$ (α 是一控制振幅强度的常数)，然后将它嵌入原始产品 x 的信息码流中：$x_i = x_i + \alpha_i w'_i$。

6.5.4 零知识证明协议下水印的认证

任何时候，Owner 都能够揭示构造的认证水印的集合信息以及证明集合中每个元素的检测值，但 Owner 必须证明至少有一个水印是合法的。假如 Owner 和 User 选择在 $\hat{I}$ 中通过检测器成功发现的水印信息 w'。认证协议如下[117]。

(1) User 和 Owner 参与硬币抛掷协议，以产生 t 个位 b_i。

(2) 对所有 t 个位，Owner 完成下列两种情况中的一种：

如果 $b_i=0$，则将 B_i 发送向 User。

如果 $b_i=1$，则将 $S_i=(B_i+B_j) \bmod (p-1)$ 发送向 User，其中 j 是 $b_j=1$ 的最小值。

(3) 对所有 t 个位，User 证明下列两种情况中的一种：

如果 $b_i=0$，那么 $a^{B_i}= m_i(\bmod\ p)$。

如果 $b_i=1$，那么 $a^{S_i}= m_i m_j(\bmod\ p)$。

(4) Owner 将 z 发送向 User：

$$z = (A+B_i) \bmod (p-1)$$

(5) User 进一步证明：

$$a^z = m m_j(\bmod\ p)$$

如果 Owner 在每一步中都能完成证明，则 User 相信 Owner 的身份。

6.5.5 对协议的补充说明

(1) 在零知识水印认证协议中，User 只是对版权进行了认证，而始终没有获得秘密身份，这一“零知识”对于用户究竟是什么？事实上，“零知识”是指注册的版权信息，由公认的版权中心 TCM 授权，具有可信性。TCM 保证对用户做诚实承诺。为了防止 Owner 在产品中嵌入伪造的版权信息，TCM 可对注册的产品及产权者的身份进行检测。另一方面，User 可能要求对产品的身份进行验证，将检测到的 w' 提交给 TCM。TCM 计算 $m= q^A$，并检验 $m\in w'$，这一点证明了 Owner 的确没有用假身份替换真实的注册身份 A 嵌入水印。TCM 将结果以“是”或“否”的形式回答 User。除此之外，不回答 User 任何询问。

(2) Owner 在每次认证中，需要重新产生一组随机数 B_i，而原来的数被丢弃。在实际水印的创建中，由于这些数对应的离散对数和 m 组成的 w' 需要嵌入数字产品中，也就是用于嵌入水印的集合是变化的，但其中存在的一个问题是，m 始终是不变的，这样就给

攻击者留有机会，因为他可以进行多次认证。从提取的众多水印中对比得到 m，尽管 m 不能得到原始的版权信息 A，但攻击者一旦知道 m，他就可以用一伪造的版权 A' 计算 $m' = q^{A'}$，连同一系列随机数，作为水印嵌入产品进行产品的重发。对该问题的解决有赖于 Owner 对水印集合的构造。在每次认证中，Owner 选取 $t-1$ 个元素连同 m 构成嵌入的水印，与前面不同的是，每次选取的 t 个元素中除了 m，有一部分可以和上一次的重复，这样的结果使得攻击者在 w' 中无法挑选出真正的 m，这是一个统计概率。t 的选取以及重复元素的个数有赖于系统对安全的要求。

(3) 在零知识水印认证协议中，为了解决来自 Owner 以及 User 的欺骗，引入了第三方 TCM，TCM 是可信的权威机构，所有在 Network 上交易的数字产品以及水印都应是在授权范围内注册过的。为了防止 Owner 以假冒身份进行网上销售或者销售假冒产品，TCM 有权时刻对网上的产品水印进行检测及跟踪。另一方面，TCM 甚至可对购买者 User 的身份进行评估。对于 TCM 是半可信的或者不可信的情况，需要在协议中增加位承诺、盲签名等辅助协议补充完成。

6.5.6 基于图同构的零知识证明在水印认证中的应用

文献[112]中提出了一个对图同构的完全零知识交互式证明系统，具体如下。

假设图 G_1 和 G_2 都有定点集 $\{1, 2, \cdots, n\}$，对图的非同构的交互式证明如下所述。

(1) 重复下列步骤 n 次。

(2) 询问者选择一个 $\{1, 2, \cdots, n\}$ 的随机置换，在置换 π 下计算图 G_1 的像 H，并发送 H 给询问者。

① 询问者选择一个随机整数 $i = 1$ 或 2，并把它发送给应答者。

② 应答者计算一个 $\{1, 2, \cdots, n\}$ 的置换 ρ，满足在 ρ 下 H 是 G_i 的像。应答者发送 ρ 给询问者(如果 $i = 1$，那么应答者定义 $\rho = \pi$；如果 $i = 2$，那么应答者定义 ρ 为 σ 和 π 的合成。这里，σ 是某一固定置换，在 σ 下 G_2 的像是 G_1)。

(3) 询问者检查在 ρ 下 H 是否是 G_i 的像。

(4) 如果在 n 轮的每一轮中 H 是 G_i 的像，那么询问者接受应答者的证明。

注意：该证明系统是完备和可靠的。很容易看到，如果 G_1 与 G_2 同构，那么询问者接受的概率为 1。如果 G_1 与 G_2 不同构，那么应答者欺骗询问者的唯一方法是他/她正确地猜出询问者在每轮中将选择的值 i，并且在通信带上写上 G_i 的一个随机同构副本。正确猜出询问者的 n 个随机询问的概率是 2^{-n}。

第7章 数字图像水印技术

本章提出了模糊熵测度算法(FEMA)检测图像中适合信息隐藏的显著的特征区域,然后将水印嵌入在这些区域的DCT系数中,以获得更高的鲁棒性;基于混沌映射将商标图像的像素在空间域中进行置乱,这个过程相当于形成了用户的密钥,也使置乱的商标信息分布随机化;提出了自适应于图像内容特征的水印嵌入算法,避免了水印化图像在平坦区域的失真;提出了利用Kalman滤波的方法对嵌入的水印进行盲检测,商标能够在随后的检测以及重构中得到可靠的恢复,以表明数字产品的版权。

7.1 图像压缩

数字图像中各个像素之间都具有很大的相关性,这种相关性造成图像信息的冗余,如空间冗余、频域空间冗余或者时间域冗余。空间冗余是因为相邻的灰度像素分布具有很强的相关性;频域空间冗余的出现是因为在多谱段图像中,不同谱段的图像对应的像素之间具有很强的灰度相关性;而时间域冗余则是因为对连续的图像而言,相近两帧之间的像素灰度同样具有很强的相关性。

数字图像中的像素灰度并不是均匀出现的,如果每个像素灰度都用同样的长度表示,就会出现冗余,即图像的信息熵冗余。此时如果把出现次数比较多的灰度值用一个比较短的编码表示,而出现次数比较少的灰度值用一个相对而言长度较长的编码表示,也有可能使得整个图像的编码总长度变短。

数字图像能量在频域的分布同样也是不均匀的。图像变换到频域后,大部分能量集中在频率比较低的部分,中频和高频的部分能量与低频部分相比较少。根据这一特点,可以先把图像变换到频域,对变换得到的频域信号进行处理,能量较小的高频分量用较短的编码表示,而能量较大的低频分量用较长的编码表示,通过这样的方式同样可提高编码的效率。

7.2 JPEG图像压缩标准

7.2.1 JPEG压缩基本系统编码器

JPEG压缩是有损压缩,它利用人的视觉系统的特性,将量化和无损压缩编码结合去除视觉的冗余信息和数据本身的冗余信息。基于基本系统的JPEG压缩编码器框图如

图 7-1 所示。

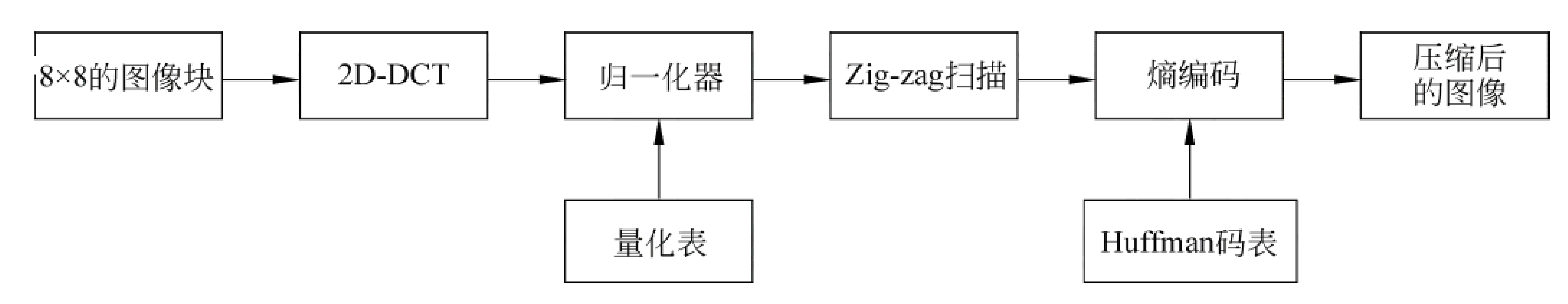


图 7-1 基于基本系统的 JPEG 压缩编码器框图

(1) 图像预处理，将 RGB 图像转为 YCrCb 颜色空间。

(2) 图像的像素点按照 8×8 块进行采样，并把采样得到的无符号数值减去固定的偏移变成有符号的数值。

(3) 2D-DCT，对第一步得到的 8×8 块的有符号数值进行 2D-DCT(二维离散余弦变换)，得到相应的 2D-DCT 系数。

(4) 量化，把步骤(2)得到的 2D-DCT 系数根据 JPEG 提供的量化表进行量化，得到相应的量化系数。

(5) Zig-zag 扫描，把步骤(3)得到的量化系数进行 Zig-zag 扫描。

(6) 熵编码。扫描之后的量化系数包括直流系数和交流系数，对直流系数进行差分预测编码，而对交流系数进行 Huffman 编码。

7.2.2 图像空间转换

JPEG 采用的是 YCrCb 颜色空间，而 BMP 采用的是 RGB 颜色空间，要想对 BMP 图片进行压缩，首先需要进行颜色空间的转换。YCrCb 颜色空间中，Y 代表亮度，Cr、Cb 则代表色度和饱和度(也有人将 Cb、Cr 两者统称为色度)，三者通常以 Y、U、V 表示，即用 U 代表 Cb，用 V 代表 Cr。RGB 和 YCrCb 之间的转换关系如下。

$$\begin{cases} Y = 0.299R + 0.587G + 0.114B \\ Cb = -0.1687R - 0.3313G + 0.5B + 128 \\ Cr = 0.5R - 0.418G - 0.0813B + 128 \end{cases} \tag{7-1}$$

一般来说，C 值(包括 Cb、Cr) 应该是一个有符号的数字，但这里通过加上 128，使其变为 8 位无符号整数，从而方便数据的存储和计算。

$$\begin{cases} R = Y + 1.402(Cr - 128) \\ G = Y - 0.34414(Cb - 128) - 0.71414(Cr - 128) \\ B = Y + 1.772(Cb - 128) \end{cases} \tag{7-2}$$

7.2.3 采样

研究发现，人眼对亮度变换的敏感度要比对色彩变换的敏感度高很多。因此，可以认为 Y 分量要比 Cb、Cr 分量重要的多。JPEG 图片中，通常采用两种采样方式：YUV411 和 YUV422，它们代表的意义是 Y、Cb、Cr 3 个分量的数据取样比例一般是 4∶1∶1 或者 4∶2∶2(4∶1∶1 的含义是：在 2×2 的单元中，本应分别有 4 个 Y、4 个 U、4 个 V 值，用

12B 存储。经过 4∶1∶1 采样处理后，每个单元中的值分别有 4 个 Y、1 个 U、1 个 V，只用 6B 就可以存储了）。这样的采样方式虽然损失了一定的精度，但也在人眼不太察觉到的范围内，减小了数据的存储量。当然，JPEG 格式里也允许将每个点的 U、V 值都记录下来。

由于后面的 DCT 是对 8×8 的子块进行处理，因此，在进行 DCT 之前必须把源图像数据进行分块。源图像中每点的 3 个分量是交替出现的，首先把这 3 个分量分开，存放到 3 张表中，然后由左及右、由上到下依次读取 8×8 的子块，存放在长度为 64 的表中，即可以进行 DCT。注意，编码时程序从源数据中读取一个 8×8 的数据块后，进行 DCT、量化、编码，然后再读取、处理下一个 8×8 的数据块。

JPEG 编码是以每 8×8 个点为一个单位进行处理的。所以，如果原始图片的长宽不是 8 的倍数，就需要先补成 8 的倍数，使其可以一块块的处理。将原始图像数据分为 8×8 的数据单元矩阵之后，还必须将每个数值减去 128，然后一一代入 DCT 公式，即可达到 DCT 的目的。图像的数据值必须减去 128，是因为 DCT 公式所接受的数字范围是－128～127。

7.2.4　DCT

静止图像压缩标准 JPEG 就是基于 DCT 的压缩标准。离散余弦变换在图像处理中占有非常重要的位置，尤其是在图像的变换编码中有非常成功的应用。离散余弦变换本质上是傅里叶变换的实数部分，但是和傅里叶变换相比，它具有更强的信息集中能力。对于大多数自然图像，离散余弦变换能将其主要信息通过少量系数表示，因而具有较高的编码效率。

一维 N 点离散余弦变换（DCT）的定义和矩阵表示形式如式(7-3)所示。

$$\begin{cases} y(k) = H_k \sqrt{\dfrac{2}{N}} \sum_{n=0}^{N-1} x(n) \cos \dfrac{(2n+1)k\pi}{2N} \\ y(k) = Hx(n) \end{cases} \tag{7-3}$$

式(7-3)中，$n,\ k = 0, \cdots, N-1$，系数 H_k 为：$H_0 = 1/\sqrt{2}$，当 $k \neq 0$ 时，$H_k = 1$ 。二维 N 点 DCT 的定义和矩阵表示如式(7-4)所示。

$$Y_{UV} = \frac{2}{N} H_U H_V \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} X_{ij} \cos \frac{(2j+1)v\pi}{2N} \cos \frac{(2i+1)u\pi}{2N} \tag{7-4}$$

JPEG 压缩中采用的 2D-DCT 一般是 8 点 DCT，得到的 2D-DCT 系数是一个 8×8 的矩阵，矩阵的第一个数据称为 DC 系数，剩余 63 个数据称为 AC 系数。

7.2.5　量化

经过 DCT 之后，一个 8×8 的像素矩阵便转换成 8×8 的频域矩阵，低频分量分布在 8×8 数据的左上角，高频分量分布在右下角。但 DCT 本身并不能实现码率压缩，64 个像素值仍然得到 64 个系数，而且还增加了比特数。量化是对经过 DCT 得到的 64 个 DCT 系数按比例缩小，并四舍五入取其整数值的一个过程。它在图像文件品质和压缩比例之间做一个平衡，在保证一定的图像质量的前提下，舍掉图像中对视觉效果影响不大的

信息。

JPEG 标准中的量化过程是对 64 个频域系数除以各自的量化步长，得到的量化结果四舍五入即为量化系数。量化步长存放于量化表中，量化表是一个 8×8 的矩阵，与 DCT 系数一一对应，它是控制 JPEG 压缩比的关键因素。

由于人眼视觉系统的频率响应随空间频率的增加而下降，即人眼对高频分量远不如对低频分量敏感，而且图片的点与点之间会有一个色彩过渡的过程，低频分量集中了大部分图像信息，所以可以将人眼视觉系统不太敏感的高频分量舍弃。鉴于此，低频分量的量化系数对应的量化步长较小，相应的失真也小，所包含的信息损失较少，高频分量的量化系数对应的量化步长较大，信息损失较大，但是视觉效果上不会有很大的变化。JPEG 压缩标准中给出了推荐量化表，因为本文仅对灰度图像进行压缩，所以只使用到亮度量化表，表 7-1 即 JPEG 推荐亮度量化表，表 7-2 即 JPEG 推荐色度量化表。

表 7-1　JPEG 推荐亮度量化表

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

表 7-2　JPEG 推荐色度量化表

17	18	24	47	99	99	99	99
18	21	26	66	99	99	99	99
47	66	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99

这两张表依据心理视觉阈制作，对 8b 亮度和色度的图像的处理效果较好。量化表是控制 JPEG 压缩比的关键，这个步骤除掉了一些高频量，损失了很多细节信息。但事实上，人眼对高频信号的敏感度远没有对低频信号那么敏感。所以，处理后的视觉损失很小。从上面的量化表也可以看出，低频部分采用了相对较短的量化步长，而高频部分则采用了相对较长的量化步长，这样做也是为了在一定程度上得到相对清晰的图像和更高的压缩率。另一个重要原因是，所有图片的点与点之间会有一个色彩过渡的过程，而大量的

图像信息都包含在低频率空间中，经过 DCT 处理后，高频率部分将出现大量连续的零。

7.2.6　Zig-zag 扫描

经过量化之后得到的量化系数矩阵，非零系数一般集中在矩阵的左上方，右下方的高频分量多数变为 0。由于在 FPGA 中数据存储是线性存储的，如果将量化系数矩阵按行存储，那么低频分量和高频分量打乱，无法表示其各自的相关性。所以，JPEG 标准中规定采用 Zig-zag 顺序存储量化系数，即从左上角开始，以“之”字形方式扫描到右下角，把二维矩阵转换为一维数据序列，这样也把高频分量的 0 值连在一起，以便进行后续的熵编码。Zig-zag 的地址扫描顺序如图 7-2 所示。

0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63

图 7-2　Zig-zag 的地址扫描顺序

7.2.7　熵编码

JPEG 标准给出的熵编码的算法是 Huffman 编码。Huffman 编码的理论基础是变长编码，利用不同符号的概率分布进行不同长度的编码，从而实现数据压缩的目的。对于由量化器输出的量化系数，JPEG 采用定长和变长结合的编码方法，具体如下所示。

（1）直流（DC）系数。

由于图像中相邻的两个图像块的 DC 系数耦合性很强，所以 JPEG 对量化后的直流系数采用无失真 DPCM（Difference Pulse Code ModulaTIon）编码，即对当前 8×8 块的直流系数 $F_i(0,0)$ 和已编码的前一个 8×8 块的直流系数 $F_{i-1}(0,0)$ 的差值进行编码。假设某一个 8×8 图像块的 DC 系数值为 15，而上一个 8×8 图像块的 DC 系数为 12，则两者之间的差值为 3。

按照得到的差值的取值范围，JPEG 把差值进行分类。编码时，将 DC 系数的差值表示为“（符号 1，符号 2）”的形式，其中符号 1 是用自然二进制码表示 DC 差值所需要的最少位数，可通过查表得到。符号 2 为实际的差值。对于符号 1，采用 Huffman 编码。由于亮度和色度分量的 DC 差值统计特性差别较大，所以 JPEG 分别给出了推荐使用的 Huffman 亮度码表和 Huffman 色度码表。对符号 2，采用自然二进制码表示，即用差值的反码表示。正数的反码是它本身，负数的反码用正数的反码表示。例如，差值为 12，用“1100”表示。

(2) AC 系数的行程长度编码(RLC)。

经过 Zig-zag 扫描之后,交流系数会出现连续的零,所以 JPEG 对零交流系数进行游程长度编码,即将所有的交流系数用 00…OA 的形式表示。其中,A 代表非零值,若干连续个 0 和一个非零值 A 组成一个编码的基本单位。因此,采用行程编码(Run Length Coding,RLC)更进一步降低了数据的传输量。

JPEG 将交流系数中的非零系数同样进行分类,即用自然二进制码表示非零值所需的最小位数。于是,可以把一个基本编码单位表示为(符号 1,符号 2)的形式。其中,符号 2 表示的是非零的 AC 系数的幅值;符号 1 为(游程/类别),即游程和类别的组合,“游程”表示每个 8×8 块的 AC 系数中连 0 的长度,“类别”表示对非零系数进行自然二进制编码需要的最少位数,即对符号 2 编码的位数。

与 DC 系数的编码类似,对符号 l 采用 Huffman 编码进行编码,JPEG 同样给出了 AC 系数亮度 Huffman 码表和 AC 系数色度 Huffman 码表:对符号 2,也采用自然二进制编码。JPEG 有两种特殊情况:①当连续 0 的个数超过或者等于 16 时,符号 1 用 ZRL (F/0)表示,同时对连 0 个数重新计数;②每个 8×8 块结束时,用 EOB(0/0)表示,即块结束标志。

例如,现有一个字符串,如下所示:

57,45,0,0,0,0,23,0,−30,−8,0,0,1,000…

经过 RLC 之后,将呈现出以下形式:

(0,57);(0,45);(4,23);(1,−30);(0,−8);(2,1);(0,0)

注意,如果 AC 系数之间连续 0 的个数超过 16,则用一个扩展字节(15,0)表示 16 个连续 0。

(3) AC 系数的中间格式。

根据前面提到的 VLI 表格,对于前面的字符串

(0,57);(0,45);(4,23);(1,−30);(0,−8);(2,1);(0,0)

只处理每对数右边的那个数据,对其进行 VLI 编码:查找上面的 VLI 编码表格可以发现,57 在第 6 组中,因此可以将其写成(0,6,57)的形式,该形式称为 AC 系数的中间格式。

同样,(0,45)的中间格式为(0,6),45;(1,−30)的中间格式为(1,5),−30。

得到 DC 系数的中间格式和 AC 系数的中间格式之后,为进一步压缩图像数据,有必要对两者进行熵编码。JPEG 标准具体规定了两种熵编码方式:Huffman 编码和算术编码。JPEG 基本系统规定采用 Huffman 编码(因为不存在专利问题),但 JPEG 标准并没有限制 JPEG 算法必须用 Huffman 编码方式或者算术编码方式。

Huffman 编码:对出现概率大的字符分配字符长度较短的二进制编码,对出现概率小的字符分配字符长度较长的二进制编码,从而使得字符的平均编码长度最短。Huffman 编码的原理请参考数据结构中的 Huffman 树或者最优二叉树。

Huffman 编码时,DC 系数与 AC 系数分别采用不同的 Huffman 编码表,对于亮度和色度,也采用不同的 Huffman 编码表。因此,需要 4 张 Huffman 编码表,才能完成熵编码的工作。具体的 Huffman 编码采用查表的方式高效地完成。然而,在 JPEG 标准中没

有定义默认的 Huffman 表，用户可以根据实际应用自由选择，也可以使用 JPEG 标准推荐的 Huffman 表。或者预先定义一个通用的 Huffman 表，也可以针对一副特定的图像，在压缩编码前通过搜集其统计特征计算 Huffman 表的值。

7.3　图像水印

许多早期的工作，主要将通信领域的扩频原理应用于水印技术中[118-125]。Cox 等人提出了类似于扩频通信的方法[126]，他们用随机产生的白高斯噪声代替水印信号而嵌入在宿主图像的 DCT 块的最大非直流系数中。Hsu 和 Wu 对文献[127]中的方案加以修改，他们将水印嵌入在宿主图像的 DCT 的中频系数中[126]，而且还将这一方案推广到基于 MPEG 的视频水印中[128]。和其他方法不同，Tao 和 Dickinson 使用人类视觉的各种隐蔽效果进行水印的嵌入[129]。其他的在 DCT 域中的嵌入方案有文献[130-134]中介绍的方案。Xia 等人提出了使用离散小波变换的分级的扩频水印方法[135,136]，类似的一些还有文献[137，138]等介绍的方法。S. Pereira 等人提出了基于 FFT(快速离散傅里叶变换)域的对于旋转等几何攻击鲁棒的水印方案[139-142]。Podilchuk 和 Zeng 提出了对文献[126]介绍的方法扩展的水印方法[143-145]，他们结合了人类视觉系统(HVS)提高水印的不可视性和鲁棒性[146]。Tirkel 等人提出了灰度图像的水印算法[147]，但这种水印算法不适合于对鲁棒性要求高的应用场合。Hus 将二进制的版权图案，而不是随机的伪随机信号嵌入在图像中[148,149]，该方案的缺点是在水印检测时需要原始图像。J. R. Smith 等人利用信息论的方法分析和评估隐藏信道性能[150-153]，运用信息理论的基本原理估计图像中可以改变的信息量，也就是水印信道的理论容量，建立了水印信道的模型，分析了加性噪声下水印的容量，但这样获得的水印容量只能是一种理论参考。Teddy 提出了在不使用原始数据的情况下水印的相关检测算法[154-157]。Juan R. 等人提出了水印的统计分析模型，利用假设检验的方法对水印进行检测[158]。

总结以上提及的图像水印方案，在构造基于自适应于图像内容的鲁棒水印方面，众多算法采取直接提取图像的特征系数加入水印，而在对特征系数的改变上则使用 HVS 或者按照子信道最大容量等的算法确定水印的权值，这样，避免在图像的平坦区域由于加入水印而出现失真。也有一些学者提出了水印应该嵌入在那些具有显著特征的图像像素上，但很少有人明确提出如何针对不同的图像检测出这些显著的特征点。针对以上存在的问题，我们在设计的水印方案中提出了新的设计思路和有效的算法。

7.4　图像水印设计方案

7.4.1　图像水印化模型

选择在图像的 DCT 域嵌入水印，主要是因为 DCT 域提供了一个不同频率和图像能量之间的分布情况，而水印可选择适当的 DCT 域中的频段嵌入。详细的水印嵌入模型

如图 7-3 所示。

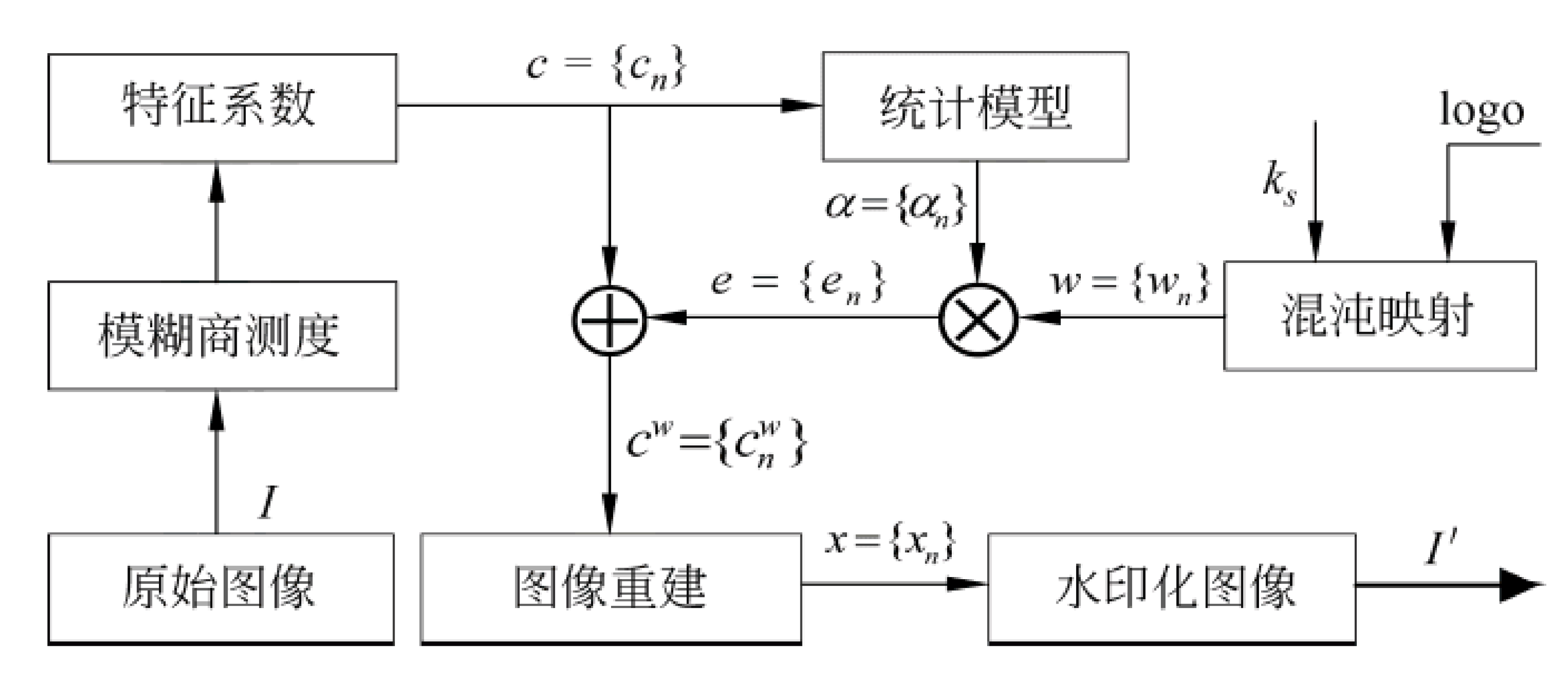


图 7-3　详细的水印嵌入模型

I 代表原始图像。

I'代表水印化的图像。

$c=\{c_n\}$为数字图像 DCT 的变换系数。

logo 为商标或者有意义的明文或者用户的 ID 号。

$\alpha=\{\alpha_n\}$为水印的嵌入系数，调节水印嵌入的强度。

$e=\{e_n\}$为调制后的水印序列。

k_s 为用户的私钥，这种私钥在水印方案中可能指秘密的参数的集合。

$c^w=\{c_n^w\}$为水印化的 DCT 系数。

$x=\{x_n\}$为最终形成的水印化的数据。

I'代表水印化的图像。

在图像水印的嵌入模型中，原始的版权信息，如用户的商标或者注册的 ID 序列通过私钥(加密)混沌映射，得到二进制随机置乱的水印 $w=\{w_n\}$序列，然后被嵌入到从原始数字图像 I 中采样出的特征集合 $c=\{c_n\}$中。这里，特征集合的元素是数字图像的相关的 DCT 变化系数。水印化系数在图像中的空间分布由模糊熵确定，也就是在嵌入商标前，首先使用模糊熵测度算法检测图像中适合信息隐藏的那些显著的特征区域，然后将水印嵌入在这些区域的 DCT 块的系数中，以获得更高的鲁棒性。

7.4.2　基于 FEMA 算法的图像特征的提取

构造鲁棒性的水印能够有效抵抗如压缩、剪裁、噪声污染等其他类型的攻击。结合图像压缩编码的特点，将需要嵌入的信息分布在图像中具有显著特征的边缘周围以及纹理化的区域，其原因在于这些部分的频率成份丰富，数值变化明显，相对于平滑区域，HVS 对于发生在这些高亮度区域中的失真不十分敏感[159]，因而数据可改变的容量相对要大。所以，在水印嵌入前，需要对原始图像在空间域中的特征分布进行检测。本书提出了基于模糊熵[160]的边缘检测算法，其定义如下。

设 $I=\{x(i,j),0<i\leqslant M,0<j\leqslant N,x(i,j)\in\{0,1,\cdots,G-1\}\}$ 表示大小为 $M\times N$ 的数字图像，$x(i,j)$是坐标(i,j)处像素的灰度值，$G=256$。将图像中像素的灰度归一化到$[0,1]$区间，仍记作 $x(i,j)$为以图像的灰度级为讨论域，定义一个具有某种特征的模糊集合，其隶属度如下。

$$u_m(x(i,j)) = \frac{1}{1 + |x(i,j) - m| / C} \tag{7-5}$$

式(7-5)表示了图像中像素与其所属区域的隶属程度，一个像素与其所属区域特征值的差异越小，该像素的隶属度越大；反之，则该像素的隶属度越小。式中，C 为常数，以保证 $0.5 \leqslant u_m(x(i,j)) \leqslant 1$，也就是期望图像中任一像素的隶属度不小于 0.5。在上述模糊集合上定义一个模糊熵[160]如下。

$$\begin{aligned} H_m[u_m(x(i,j))] = & - u_m(x(i,j))\log_2[u_m(x(i,j))] \\ & - [1 - u_m(x(i,j))]\log_2[1 - u_m(x(i,j))] \end{aligned} \tag{7-6}$$

模糊熵随像素 $x(i,j)$ 的大小而变化的曲线如图 7-4 所示。可以看出，当灰度值 $x(i,j)=m$，$(m \in [0,1])$ 时，模糊熵最小，且在 $x(i,j)=m$ 附近具有对称性。

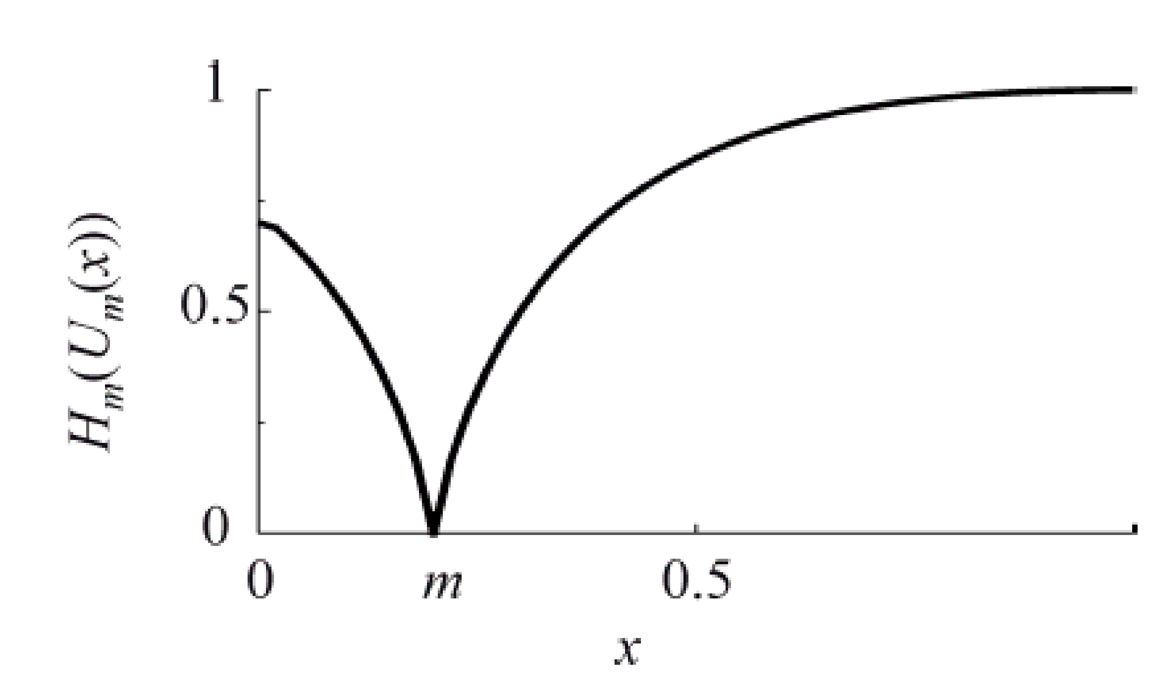


图 7-4　模糊熵随 x 的变化曲线

一般地，图像中具有显著特征点的邻域内的灰度分布和其他点邻域内的灰度分布不同，平坦点的邻域内通常只有一种灰度分布，具有显著特征点的邻域内灰度分布的差异较大。本文定义一种模糊熵测度表征这种灰度分布的有序性。

在图像的灰度值矩阵中取一个大小为 $n \times n$，中心在 (i,j) 的窗口 $W_n(i,j)$

$$W_n(i,j) = \begin{bmatrix} & \vdots & \vdots & \vdots & \\ \cdots & x(i-1,j-1) & x(i,j-1) & x(i+1,j-1) & \cdots \\ \cdots & x(i-1,j) & x(i,j) & x(i+1,j) & \cdots \\ \cdots & x(i-1,j+1) & x(i,j+1) & x(i+1,j+1) & \cdots \\ & \vdots & \vdots & \vdots & \end{bmatrix} \tag{7-7}$$

则在该窗口 $W_n(i,j)$ 上，可定义一个基于模糊熵的邻域一致性信息测度 $R(i,j)$ 为

$$R(i,j) = \frac{1}{n \times n} \sum_{k=-(n-1)/2}^{(n-1)/2} \sum_{l=-(n-1)/2}^{(n-1)/2} H_m[u_m(x(i+k, j+l))] \tag{7-8}$$

在式(7-8)中，令 $m = x(i,j)$，则当窗口中的其他灰度值和窗口中心 (i,j) 处的灰度值 $x(i,j)$ 相等或接近时，表明该像素处于图像的平滑区域，模糊熵 $R(i,j)$ 为零或较小。反之，当该像素处于图像的特征显著，或者能量变化较大的区域（边缘、纹理）时，则 $R(i,j)$ 较大。本质上，$R(i,j)$ 反映了图像变化的不定性，这种性质为在图像中寻找适合隐藏水印信息的区域提供了理论上的一种依据。为了和基于图像 8×8 分块处理的水印算法一致，可定义第 k 个图像块的信息测度为

$$R_k = \frac{1}{64} \sum R(u,v) \quad u,v = 1,2,\cdots,8 \tag{7-9}$$

7.4.3 商标置乱及水印产生

我们使用混沌映射的方法，将商标进行随机置乱。置乱的目的有两个：一是排列有序的商标经过置乱后，服从伪随机序列的概率分布的特点；另一个原因是，从水印系统的安全考虑，因为注册的商标本身是可识别或者说是可读的，直接将注册商标加入图像中，一旦有关商标信息被泄露，那么，对于攻击者，同样可使用相同的商标采用不同的手法进行版权的伪造。因此，商标的置乱无论对水印的嵌入，还是检测，以及整个系统的安全，都是很重要的一个环节。从技术上讲，置乱可以理解为一种信号的映射，置乱使用的参数被认为是版权者的密钥，只有版权者唯一掌握密钥，才能对商标进行秘密的隐藏和正确的检测。本方案采用 G. Voyatzis 等人在文献[151,161]中使用的混沌映射的算法实现对商标的置乱。该映射算法可叙述如下。

考虑一二维向量在空间域的“自同构”变换，可以用数学上的一映射表示：

$$A: U \to \boldsymbol{U}, \quad U = [0,1) \times [0,1) \subset \boldsymbol{R}^2 \tag{7-10}$$

而且可由下面的公式定义

$$\boldsymbol{r}' = \boldsymbol{A}\boldsymbol{r}(\mathrm{mod}\ 1), \quad \begin{pmatrix} x_{n+1} \\ y_{y+1} \end{pmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} (\mathrm{mod}\ 1) \tag{7-11}$$

这里，$a_{i,j} \in \boldsymbol{Z}$，$\det \mathbf{A} = 1$，而且 $\mathbf{A}$ 的特征值 $\lambda_{1,2} \notin \{-1,0,1\}$。在一点 $\boldsymbol{r}_0 \in \boldsymbol{U}$ 上对 $\boldsymbol{A}$ 的迭代将形成一动态的系统 $A^{(n)}: U \to \boldsymbol{U}$，具体如下。

$$\boldsymbol{r}_{n+1} = \boldsymbol{A}^n \boldsymbol{r}_0 (\mathrm{mod}\ 1), \quad \text{或者} \quad \boldsymbol{r}_{n+1} = \boldsymbol{A}\boldsymbol{r}_n (\mathrm{mod}\ 1) \tag{7-12}$$

这里，$n = 0, 1, 2, \cdots$。

对该映射的几个特性总结如下。

(1) 因为 $a_{i,j} \in \boldsymbol{Z}$，$\det \mathbf{A} = 1$，所以这种“同构”迭代的逆存在，即存在矩阵 $\mathbf{A}$ 的逆阵 $\mathbf{A}^{-1}$，使

$$\boldsymbol{r} = \boldsymbol{A}^{-1} \boldsymbol{r}' (\mathrm{mod}\ 1) \tag{7-13}$$

同样，$\boldsymbol{r}_0 = (\mathbf{A}^{-1})^n \boldsymbol{r}_{n+1} (\mathrm{mod}\ 1)$ 或者 $\boldsymbol{r}_{n+1} = \boldsymbol{A}\boldsymbol{r}_n (\mathrm{mod}\ 1)$。

(2) $\lambda_{1,2} \notin \{-1,0,1\}$ 保证映射的混沌性。

(3) 对式(7-8)进行迭代，所有点 $o(\boldsymbol{r}_0) = \{\boldsymbol{r}_0, \boldsymbol{r}_1, \boldsymbol{r}_2, \cdots\}$ 构成的集合是系统的一个采样轨道(Orbit)，在一特殊的(Anosov Differomophisms)类中构成自同构，这种同构在混沌系统中符合局部不稳定、各态历经并且弱相关。粗略地讲，如果 $\mathbf{V}_0$ 是 $\boldsymbol{U}$ 上的一个密集，那么在映射 $A^{(n)}$ 下的 $\mathbf{V}_0$ 的像 $\mathbf{V}_n$ 随机地扩展到整个 $\boldsymbol{U}$ 的空间上。

(4) 在有限空间上，初始位置 r_0 具有有理数坐标(充分必要条件)条件下，则轨迹 $o(\boldsymbol{r}_0) = \{\boldsymbol{r}_0, \boldsymbol{r}_1, \boldsymbol{r}_2, \cdots\}$ 是周期的，即存在一迭代次数 T 能够使 $\boldsymbol{r}_0 = \boldsymbol{r}_T$。

(5) 轨道的演变唯一地依赖于矩阵的特征值 λ_1(或者 λ_2)[151]。因此，自同构是一个单参数的系统。

$$trace\ \mathbf{A} = a_{11} + a_{22} = f(\lambda_1)$$

在版权保护中，用户的商标(二进制图像)需要预先进行随机的置乱，成为像噪声一样的随机信号，这种随机信号将被当作水印嵌入到多媒体数据中。基于对以上“自同构”映射及其性质的研究，可据此建立图像水印的置乱映射：

$$A_N(k):\begin{pmatrix}x_{n+1}\\y_{n+1}\end{pmatrix}=\begin{pmatrix}1 & 1\\k & k+1\end{pmatrix}\begin{pmatrix}x_n\\y_n\end{pmatrix}(\mathrm{mod}\ N) \tag{7-14}$$

其中，(x_n,y_n)、(x_{n+1},y_{n+1})分别为图像中某一点迭代前以及迭代后的位置坐标，$N,k\in[1,N)\subset\mathbf{Z}$。这里，矩阵的最大特征值可通过计算确定为 $\lambda_1=1+0.5(k+(k^2+4k)^{1/2})$，而且对于任何 $k>0$，都是正的实数。

映射式(7-10)可直接用于正方形(还可以推广到非正方形的情况)的图像 I 或者图像中的一个 $N\times N$ 大小的正方形子块 $U^0\subset I$。通过迭代过程可产生一系列混合的块

$$U^{(i)}=A_N^i(k)U^{(0)},\quad i=1,2,\cdots,T-1 \tag{7-15}$$

这里，T 是重现的次数(周期)。从 $U^{(n)}$ 对 U^0 的重建可通过应用一个逆的自同构的过程完成，通常情况下存在

$$U^{(0)}=A_N^{-n}(k)U^{(n)}=A_N^{P-n}(k)U^{(n)} \tag{7-16}$$

实际应用中，假设原始的版权商标是一二进制的大小为 $S_1\times S_2$ 的 BMP 图像，表示为

$$\mathrm{LOGO}=\{L_{k,l}\mid 0\leqslant k<S_1,0\leqslant l<S_2,L_{k,l}\in\{0,1\}\} \tag{7-17}$$

原始图像或者图像的子块的大小为 $N\times N$，可表示为

$$I=\{L_{k,l}\mid 0\leqslant k,l<N,L_{k,l}\in\{0,1,\cdots,G\}\} \tag{7-18}$$

G 为图像的最大灰度值。假设条件 $S_1\times S_2<<N\times N$ 成立。将式(7-16)直接应用于式(7-17)可获得置乱的商标图像

$$\mathrm{LOGO}'\leftarrow A_N^i(k)\ \mathrm{LOGO},\quad i=1,2,\cdots,T-1 \tag{7-19}$$

其中，$\mathrm{LOGO}'=\{L_{k',l'}\mid 0\leqslant k',l'<N,L_{k',l'}\in\{0,-1,1\}\}$。令

$$L_{k',l'}=\begin{cases}1, & L_{k,l}=1\\-1, & L_{k,l}=0\\0, & \text{其他}\end{cases} \tag{7-20}$$

事实上，LOGO′中只有原始商标映射来的位置上的像素是真正的置乱信息，而其他的位置的像素置零。将 LOGO′中有用的信息按照行列先后位置重新排列，得到置乱的二维水印信号 W，W 中的信息将被嵌入到从图像采样得到的显著特征中。

7.4.4　水印的嵌入算法

(1) 将亮度图像 I 分解成互不重叠的 8×8 的图像块，$I=\bigcup_{k=1}^{N}B_k(u,v)$，$(u,v)$是块中的坐标 $u,v=1,2,\cdots,8$，N 是能分成块的个数，用 FEMA 的算法对整个图像上分块的模糊熵测度进行统计检测，设置门限 τ 及水印标志位 b_k，$k=1,2,\cdots,N$，检测 R_k，如果 $R_k>\tau$，则置 $b_k=1$，否则 $b_k=0$。τ 的值可根据嵌入水印需要块的最大数量而自适应地调节。

(2) 选择 BMP 图像作为用户的商标，在商标嵌入前进行空间域的混沌映射。映射算法本身可被认为是公开的，而对于具体的应用，由于选择不同参数可获得不同的映射空间和置乱效果，因此参数 k、d、p、S 可被认为是用户的密钥。同样，将置乱后的 w 分成互不重叠的 N_1 个 4×4 的分块而嵌入到相应的 DCT 块中。

(3) 水印的嵌入基于图像的分块，选择模糊熵测度大于门限的 N_1 个图像块嵌入水印，即若 $b_k=0$，则保持原始的图像块不变；若 $b_k=1$，对相应的图像块进行 DCT，

$C_k(u',v')=DCT\{B_k(u,v)\},u',v'=1,2,\cdots,8$。

(4) 计算相应的水印权值 $\alpha_k(u,v)$。$\alpha_k(u,v)$随着块的特征系数而变化，在具体水印嵌入块中，首先对局部的变化方差 $\sigma_k(u,v)$进行估计：

$$\sigma_k(u,v)=\frac{1}{2W+1}\sqrt{\sum_{i=-W}^{W}\sum_{j=-W}^{W}(p_k(u+i,v+j)-\overline{p_k(u,v)})^2}$$

其中，

$$\overline{p(u,v)}=\frac{1}{(2W+1)^2}\sum_{i=-W}^{W}\sum_{j=-W}^{W}P_k(u+i,v+j)$$

且令

$$\alpha_k(u,v)=\lambda R_k\sigma_k(u,v) \tag{7-21}$$

(5) 使用 $\alpha_k(u,v)$加权相应的水印 $w_k(u,v)$，块中水印化的系数 $C_k^w(u,v)$的计算如下

$$C_k^w(3+t,3+v)=C_k(3+t,3+v)+\alpha_k(3+t,3+v)w_k(t,l) \tag{7-22}$$

这里，$t,l=1,2,\cdots,4$，代表水印图像的第 k 个 4×4 分块中的坐标。

(6) 在选择的块中嵌入水印的信息后，用 $C_k^w(u,v)$代替 $C_k(u',v')$，然后进行逆 DCT，$B_k^w(u',v')=IDCT\{C_k^w(u,v)\}$，各个水印化的分块重新排列，最终形成水印化的亮度图像。

7.4.5 水印的检测及商标的重构

1. 一般的相关检测原理

前面对水印的检测已提出很多种方法，在这些方法中，有需要原始图像数据的方法，也有不需要原始图像数据的方法，为此，也将水印的检测区分为"公钥水印"和"私钥水印"。在检测中不需要原始的产品数据应该说更符合水印的实际应用需求。这里简要介绍水印的相关检测，图 7-5 为相关检测模型。

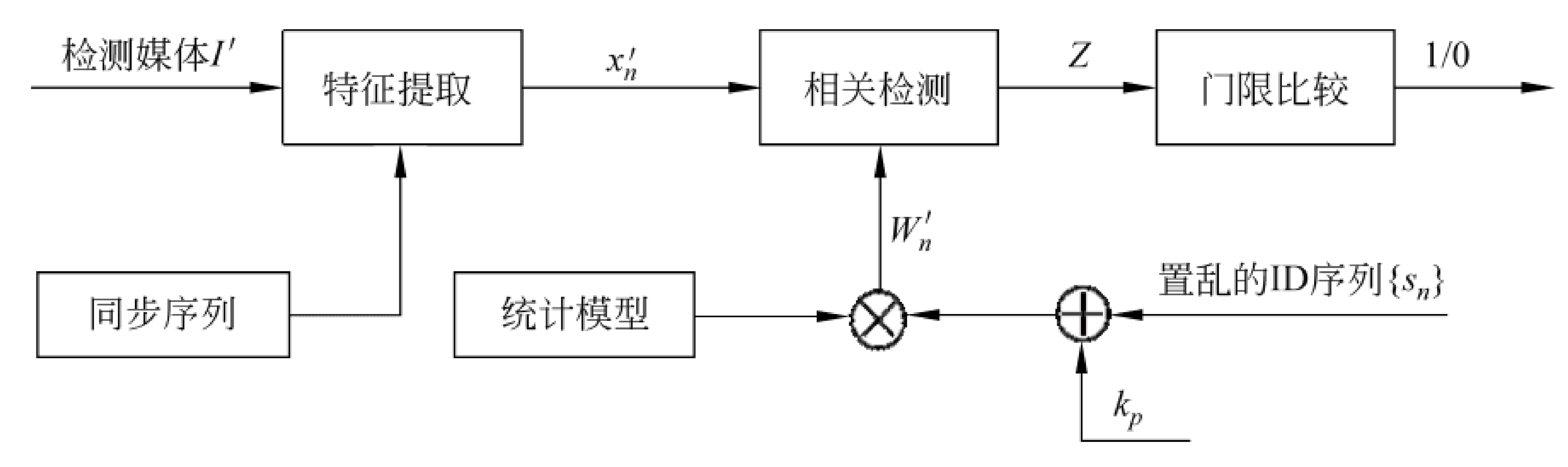


图 7-5 水印的相关检测模型

在水印化的图像未经任何失真的情况下，由图 7-3 可得

$$x'_n=c_n+e_n=c_n+\alpha_n w_n \tag{7-23}$$

假如水印化的图像没有受到任何失真，设参考的水印序列为 w'_n，利用相关峰值检测时，相关函数

$$\begin{aligned}\phi_{x'_n w'_n}(l)&=E[(c_n+\alpha_n w_n)w'_{n-l}]=E[(c_n+\alpha_n w_n)w'_{n-l}]\\&=\phi_{cw'}(l)+\alpha_n\phi_{ww'}(l)\end{aligned} \tag{7-24}$$

在文献[162,163]中，假设 $w=\{w_n\}$为随机序列，其分布符合$(0,\sigma^2)$。c_n、α_n 和 w_n 分别为平稳的且相互之间独立的统计序列，因此式(7-24)可简化为

$$\phi_{x_n w'_n}(l) = \alpha_n \phi_{ww'}(l) \tag{7-25}$$

当 $w_n \cong w'_n$ 时，出现相关峰值；如果 $w_n \neq w'_n$，或者很大程度上不相关，则相关函数为零或者很小。实际中常常将相关器输出（设为 Z）和一设定的门限 η 相比较，如果 $Z > \eta$，则数字媒体中嵌入的水印和声明的水印相符合，否则不符合。

2. Kalman 滤波的检测原理

Kalman 滤波是 Wiener 滤波的发展[159-164]，常用于随机过程的状态参数估计，它的特点有：①其数学公式可用状态空间的概念描述；②它的解是递推计算的。考虑一动态系统，它可由描述状态向量的过程方程和描述观测向量的观测方程共同表示，分别如式(7-26)和式(7-27)所示。

$$x(n) = F(n, n-1)x(n-1) + v_1(n-1) \tag{7-26}$$

$$y(n) = C(n)x(n) + v_2(n) \tag{7-27}$$

其中，

$x(n)$ 表示系统在时刻 n 时的 $M \times 1$ 状态向量。

$F(n, n-1)$ 表示 $N \times M$ 状态转移矩阵向量。

$v_1(n-1)$ $M \times 1$ 的过程噪声向量。

$y(n)$ 表示系统在时刻 n 的 $N \times 1$ 观测向量。

$C(n)$ 表示一已知的 $N \times M$ 观测矩阵。

$v_2(n)$ $N \times 1$ 的观测噪声向量。

假设：

(1) $v_1(n)$ 和 $v_2(n)$ 均为零均值的白噪声过程，即

$$E[v_1(n)] = 0;\quad \mathrm{cov}[v_1(n), v_1(k)] = E[v_1(n)v_1^H(k)] = Q_1(n)\delta(n-k) \tag{7-28}$$

$$E[v_2(n)] = 0;\quad \mathrm{cov}[v_2(n), v_2(k)] = E[v_2(n)v_2^H(k)] = Q_2(n)\delta(n-k) \tag{7-29}$$

以上两式中，

$$Q_1(n) = \mathrm{var}(v_1(n)) = E[v_1(n)v_1^{\mathrm{T}}(n)]$$

$$Q_2(n) = \mathrm{var}(v_2(n)) = E[v_2(n)v_2^{\mathrm{T}}(n)]$$

分别为 $v_1(n)$ 和 $v_2(n)$ 的自相关矩阵。

(2) $v_1(n)$ 和 $v_2(n)$ 相互独立，即

$$\mathrm{cov}[v_1(n), v_2(k)] = E[v_1(n)v_2^H(k)] = 0,\ \forall\, n, k$$

(3) 初始状态 $x(0)$ 与 $v_1(n)$、$v_2(n)$，$n \geqslant 0$ 均不相关。

如果没有两个噪声，由式(7-26)和式(7-27)立即可求得 $x(n)$，当然就不存在估计的问题。估计问题的存在正是因为信号与噪声叠加在一起，而要估计其中的信号的真值。若暂时不考虑 $v_1(n)$ 和 $v_2(n)$，按照式(7-26)和式(7-27)得到的 $x(n)$ 和 $y(n)$ 分别用 $\hat{x}'(n)$ 和 $\hat{y}'(n)$ 表示。

$$\hat{x}'(n) = F(n, n-1)\,\hat{x}'(n-1) \tag{7-30}$$

$$\hat{y}'(n) = C(n)\,\hat{x}'(n) = C(n)F(n, n-1)\,\hat{x}'(n-1) \tag{7-31}$$

将 $\hat{y}'(n)$ 与实际观测信号的误差定义为

$$\tilde{y}(n) = y(n) - \hat{y}'(n) \tag{7-32}$$

显然，造成式(7-32)的误差是由于忽略了两个噪声。由此可见，在 $\tilde{y}(n)$ 中隐含了

$v_1(n)$和$v_2(n)$的信息，称其为系统的“新息”过程。若通过一$H(n)$加权$\tilde{y}(n)$修正式(7-30)的状态估计，则得到

$$
\begin{aligned}
\hat{x}'(n) &= F(n,n-1)\hat{x}'(n-1) \\
&\quad + H(n)[y(n) - C(n)F(n,n-1)\hat{x}'(n-1)]
\end{aligned}
\tag{7-33}
$$

将式(7-33)中参考了系统“新息”得到的估计值$\hat{x}'(n)$和实际信号$x(n)$之间的差值表示为$\tilde{x}(n)$，则

$$
\begin{aligned}
\tilde{x}(n) &= x(n) - \hat{x}(n) = F(n,n-1)x(n-1) + v_1(n) - \hat{x}(n) \\
&= [I - H(n)C(n)][F(n,n-1)(x(n-1) - \hat{x}'(n-1)) + v_2(n)] \\
&\quad - H(n)v_2(n)
\end{aligned}
\tag{7-34}
$$

如果能够求得$\tilde{x}(n)$均方误差最小条件下的$H(n)$，根据式(7-33)就可以得到$x(n)$的线性最优估计$\hat{x}(n)$。为此，定义均方误差矩阵

$$
P(n) = E\{[x(n) - \hat{x}(n)][x(n) - \hat{x}(n)]^{\mathrm{T}}\} = E[\tilde{x}(n)\tilde{x}^{\mathrm{T}}(n)] \tag{7-35}
$$

且令

$$
P'(n) = E\{[x(n) - \hat{x}'(n)][x(n) - \hat{x}'(n)]^{\mathrm{T}}\} \tag{7-36}
$$

将式(7-33)和式(7-34)分别代入式(7-35)和式(7-36)且基于前面3条假设可得到

$$
\begin{aligned}
P(n) &= [I - H(n)C(n)][F(n,n-1)P(n-1)F^{\mathrm{T}}(n,n-1) + Q_1(n)] \\
&\quad \cdot [I - H(n)C(n)]^{\mathrm{T}} + H(n)Q_2(n)H^{\mathrm{T}}(n)
\end{aligned}
\tag{7-37}
$$

$$
P'(n) = F(n,n-1)P(n-1)F^{\mathrm{T}}(n,n-1) + Q_1(n) \tag{7-38}
$$

经过系列推导(详细推导可参考文献[159])可得到一组Kalman一步递推公式：

$$
\begin{cases}
\hat{x}'(n) = F(n,n-1)\hat{x}'(n-1) + H(n)[y(n) - C(n)F(n,n-1)\hat{x}'(n-1)] \\
P'(n) = F(n,n-1)P(n-1)F^{\mathrm{T}}(n,n-1) + Q_1(n) \\
P(n) = [I - H(n)C(n)]P'(n) \\
H(n) = P'(n)C^{\mathrm{T}}(n)/[C(n)P'(n)C^{\mathrm{T}}(n) + Q_2(n)]
\end{cases}
\tag{7-39}
$$

Kalman估计$\hat{x}(n)$的一步递推法如图7-6所示。

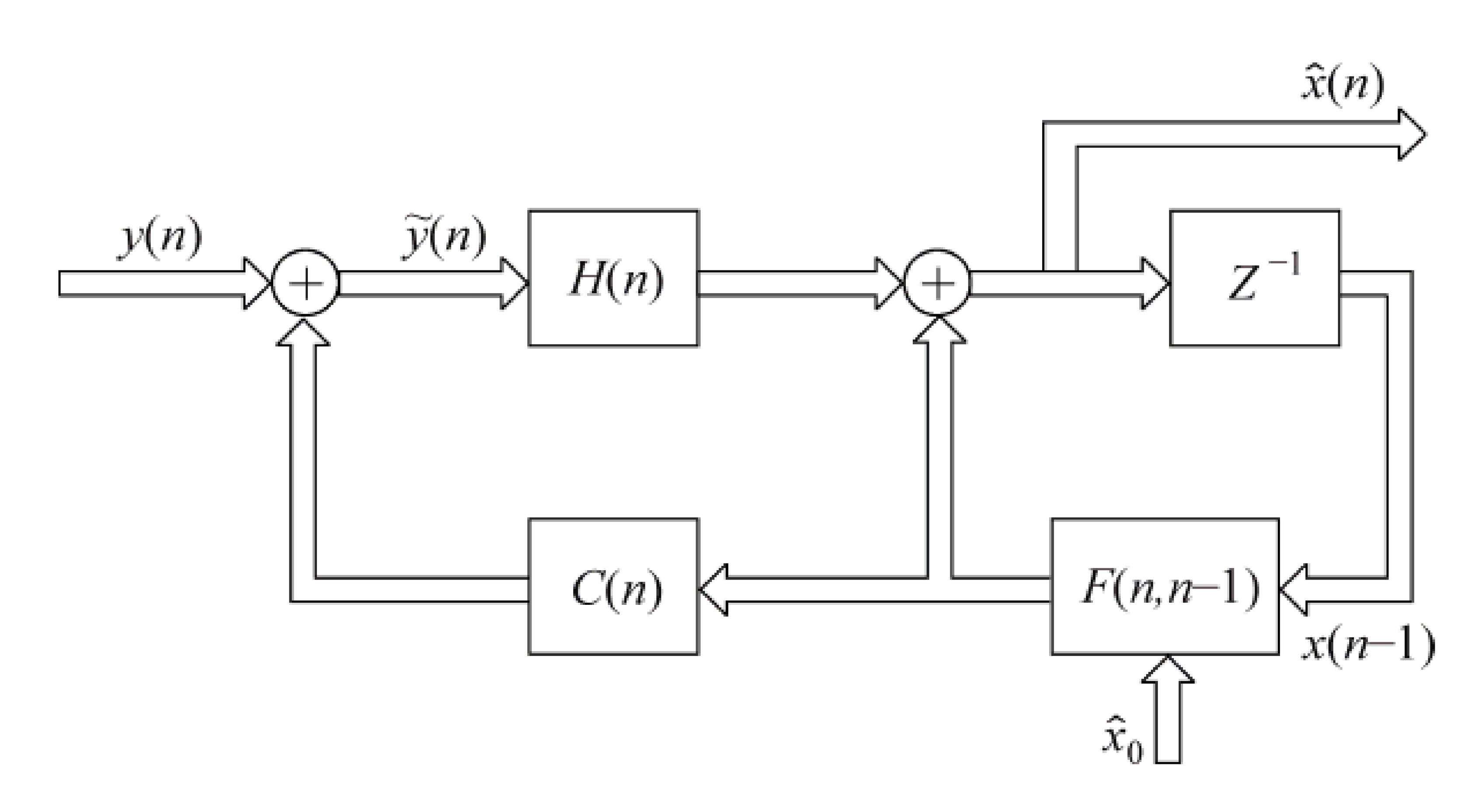


图7-6　Kalman估计$\hat{x}(n)$的一步递推法

这种递推计算方法用计算机计算十分方便，实际中可以根据已知的矩阵$F(n,n-1)$，$C(n)$，$Q_1(n)$，$Q_2(n)$以及观察到的数据$y(n)$，用递推算法得到所有的$\hat{x}(1)$，$\hat{x}(2)$，…，$\hat{x}(n)$以及$P(1)$，$P(2)$，…，$P(n)$。

3. 基于Kalman滤波的水印检测

假设插入水印后的图像信号为

$$y_{i,j}=\alpha_{i,j}w_{i,j}+x_{i,j} \tag{7-40}$$

这里，$y_{i,j}$为水印化的图像的特征数据；$x_{i,j}$为原始图像特征数据；$w_{i,j}$为内插水印信号；$\alpha_{i,j}$为从原始图像中提出的嵌入权值，它们均为二维序列。现在要求从观察到的 $y_{i,j}$ 中提取出水印（或者商标）$w_{i,j}$的估计值 $\hat{w}_{i,j}$。为了讨论的方便，我们将以上的各二维序列分别转换成一维序列向量的形式，并将式(7-36)转换为式(7-41)的形式，如下。

$$y_n=\alpha_n w_n+x_n \tag{7-41}$$

从水印化图像中估计嵌入的水印信号，相当于将原始图像数据作为噪声，即 $x_n=v_n(n)$，将式(7-37)作为检测系统的**观测方程**。而对于版权所有者，原始 w_n 是已知的，所以可以得到式(7-22)中的**过程方程**为

$$w_n=F_{n,n-1}w_{n-1} \tag{7-42}$$

其中，令式(7-26)的过程噪声 $v_1(n)=0$。

在 Kalman 过程方程和观测方程中，状态转移矩阵 $F(n,n-1)$和观测矩阵 $C(n)$是已知的，而在水印检测中，这两个参数可通过水印的产生算法和嵌入算法获得。对于真正的版权者，显然是已知的。

水印的盲检测要求在检测端不提供原始图像数据，可提供水印的参考序列。在已知参考序列的情况下，状态转移矩阵可通过式(7-42)立即获得，即

$$F_{n,n-1}=w_n w_{n-1}^{-1} \tag{7-43}$$

至于观测矩阵，尽管水印的嵌入算法可认为公开，但在不知道原始图像的情况下，这些基于图像内容的嵌入权值系数是不得而知的，如果在检测端既提供参考水印序列，又提供权值，根据式(7-41)可得

$$x_n=y_n-\alpha_n w_n \tag{7-44}$$

从式(7-44)可看出，这无异于提供了原始的图像数据(但这里需要说明的是，这种情况和提供原始图像数据还是有根本区别的，因为在这些数据中并没有含有它们采样于原始图像的确切位置信息)。为了解决该问题，使得 Kalman 预测能够在水印估计中的条件成立，在模拟实验中用权值向量 α_n 的统计均值 α 代替 α_n，这样，在预测时就不需要提供 α_n，而只提供其统计特性，也使得递推算法得到简化。对于版权所有者来说，α_n 的统计特性在此时相当于他/她的密钥的一部分。

显然，采用以上处理将会带来水印估计的误差，但只要能够将误差控制在一定范围内，这种办法就是可行的。在我们的模拟试验中给出了估计误差。最后，根据 Kalman 滤波检测原理，可以得到水印估计如下。

$$\hat{w}_n=F_{n,n-1}\hat{w}_{n-1}+H_n(w'_n-\alpha F_{n,n-1}\hat{w}_{n-1}) \tag{7-45}$$

均方误差最小条件下的 Kalman 增益方程为

$$H_n=P'_n a/(|a|^2P'_n+\sigma_{x_n}^2) \tag{7-46}$$

这里，$\sigma_{x_n}^2$为原始图像的自相关函数矩阵。事实上，在检测端是不知道的，但可通过观测数据以及参考水印序列求得。假设原始的图像数据和水印参考序列是统计独立的，由式(7-41)求 y_n 的自相关函数，则

$$\sigma_{y_n}^2=\sigma_\alpha^2\sigma_{w_n}^2+\sigma_{x_n}^2 \tag{7-47}$$

进一步，

$$\sigma_{x_n}^2 = \sigma_{y_n}^2 - \sigma_a^2 \sigma_{w_n}^2 \tag{7-48}$$

式(7-46) 中的 P'_n 可通过式(7-49)迭代

$$P'_n = |F_{n,n-1}|^2 P_{n-1} \tag{7-49}$$

而 P_n 的迭代如下

$$P_n = (I - H_n a) P'_n \tag{7-50}$$

如同式(7-35)中 $P(n)$的定义，在水印检测中，P_n 的定义如下

$$P_n = E\{[W_n - \hat{w}_n][W_n - \hat{w}_n]^{\mathrm{T}}\} = E[\tilde{w}_n \tilde{w}_n^{\mathrm{T}}] \tag{7-51}$$

将式(7-51)～式(7-54)的递推结果代入式(7-45)就可估计出嵌入的水印信号。

4. 版权商标的恢复

重新排列 Kalman 滤波估计出的嵌入水印，构成一二维向量 $\hat{w}'$。对$\hat{w}'$ 进行逆映射如下。

$$\hat{w}' \leftarrow (A_N^i(k))^{-1}\, \hat{w}' \tag{7-52}$$

将 $\hat{w}'$ 中的值替回二进制的商标值，即可获得嵌入的商标。

另一种对商标的恢复方法为可考虑用 $A_N^{T-i}(k)$ 对$\hat{w}'$ 进行逆映射，即

$$\hat{w}' \leftarrow A_N^{T-i}(k)\, \hat{w}' \tag{7-53}$$

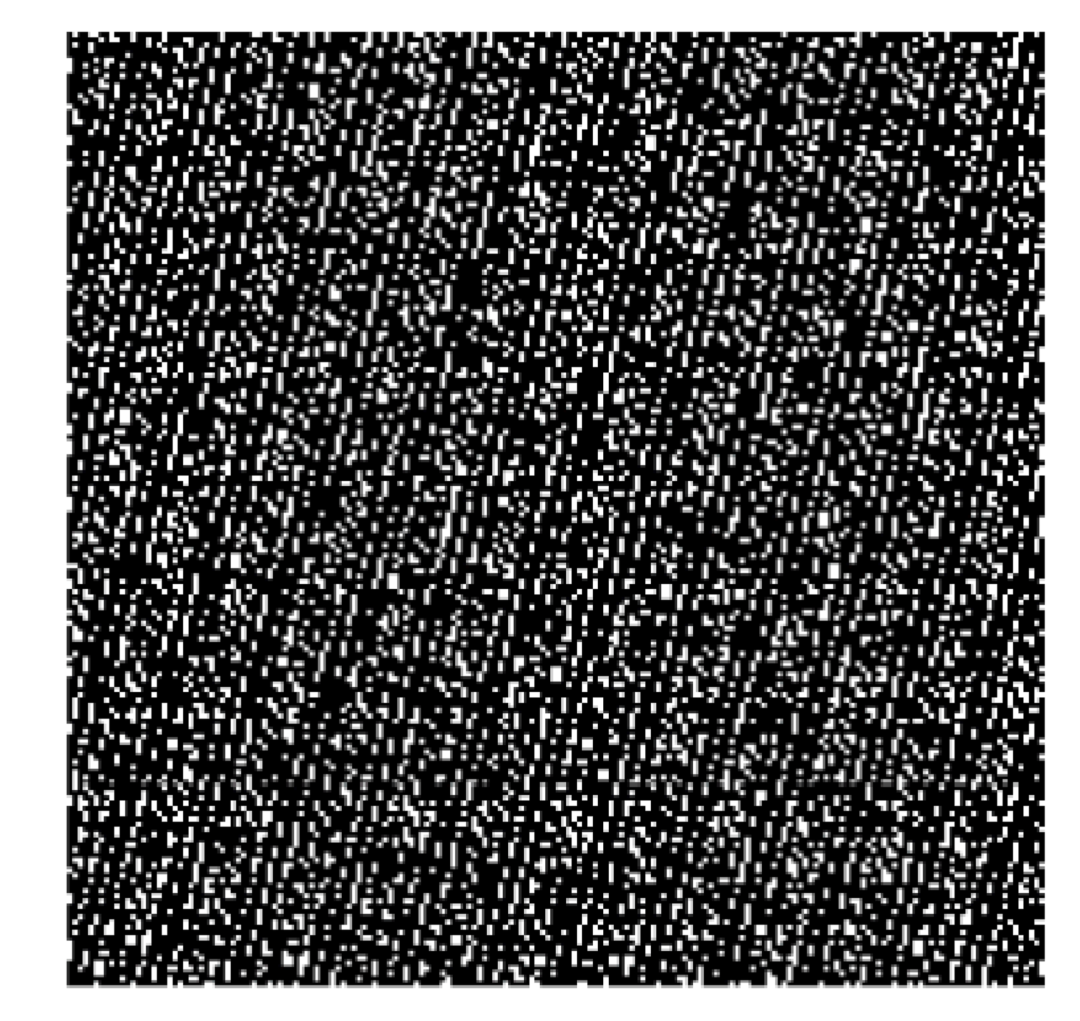
式(7-53)是对商标的恢复，具有很重要的意义。这种情况下，检测端提供的映射参数和原始嵌入的参数不同，但它们之间是对应的。因为从前面的讨论可知，这种映射为有限域的自同构映射，能够构造出这样的“公钥对”。

7.5 实验结果

在 512×512 大小的 Plane 和 Lanna 图像上进行模拟实验，选择 YAHOO!作为二进制的水印商标，其大小为 40×140。嵌入之前，先使用商标混沌映射将其在空间域中置乱，映射参数取 $k=11$，$N=188$，$n=87$，如图 7-7 所示。显然，从图 7-7(b)中的图案很难推出图 7-7(a)的原始商标。这里的映射参数还可根据需要而选择。




(a) 原始的版权商标



(b) 置乱后的商标

图 7-7　原始商标及其置乱

图 7-8 是利用模糊熵在图像上对特征的检测结果。从图 7-8(a)、(b)的检测结果可以看出，模糊熵的确反映了图像中存在的不定性，在图像的平坦区域测得的熵值很小，而在边缘和纹理变化强烈的地方，模糊熵相对大得多，这可以通过检测结果证明。使用模糊熵的目的主要是找到图像中存在的这些变性比较大的地方，这些地方的变化对人的感觉刺激相对不敏感，有利于水印信息的嵌入。



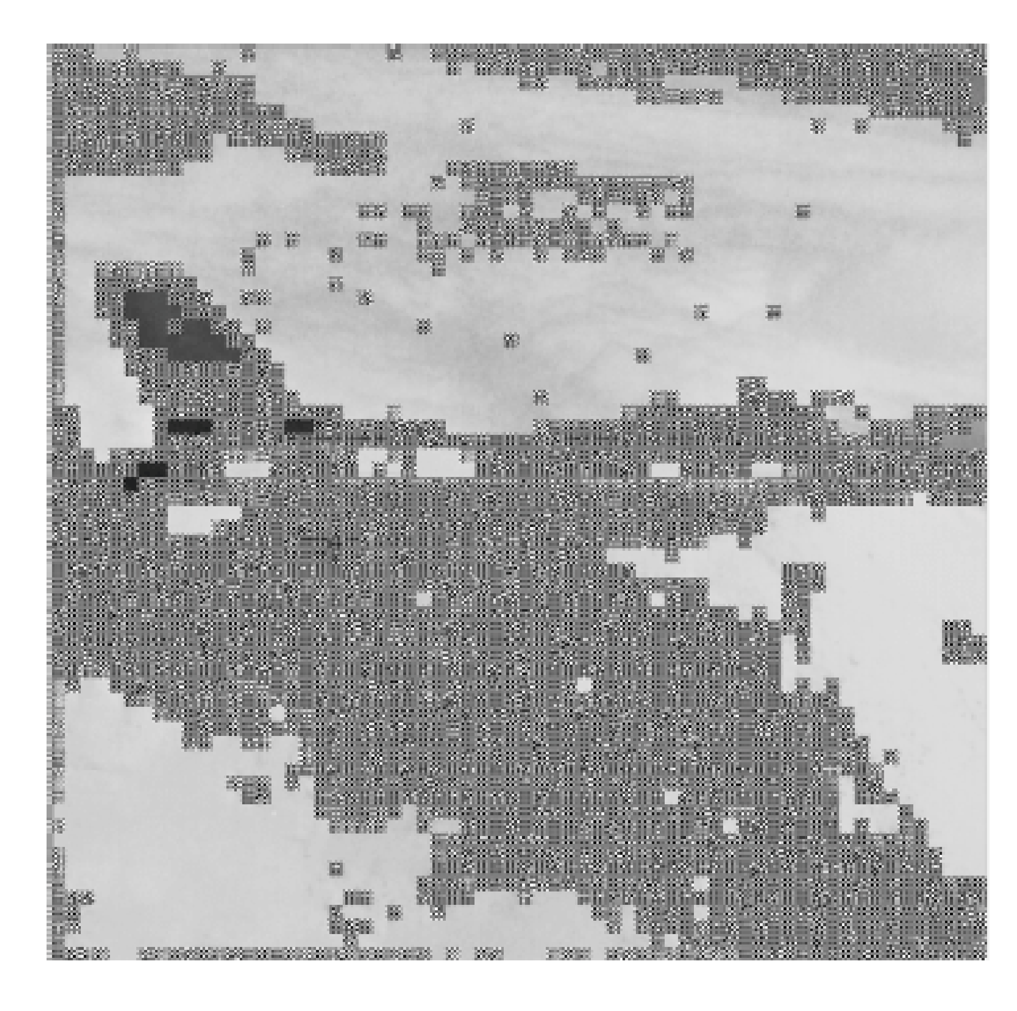
(a) Plane上的模糊熵检测结果



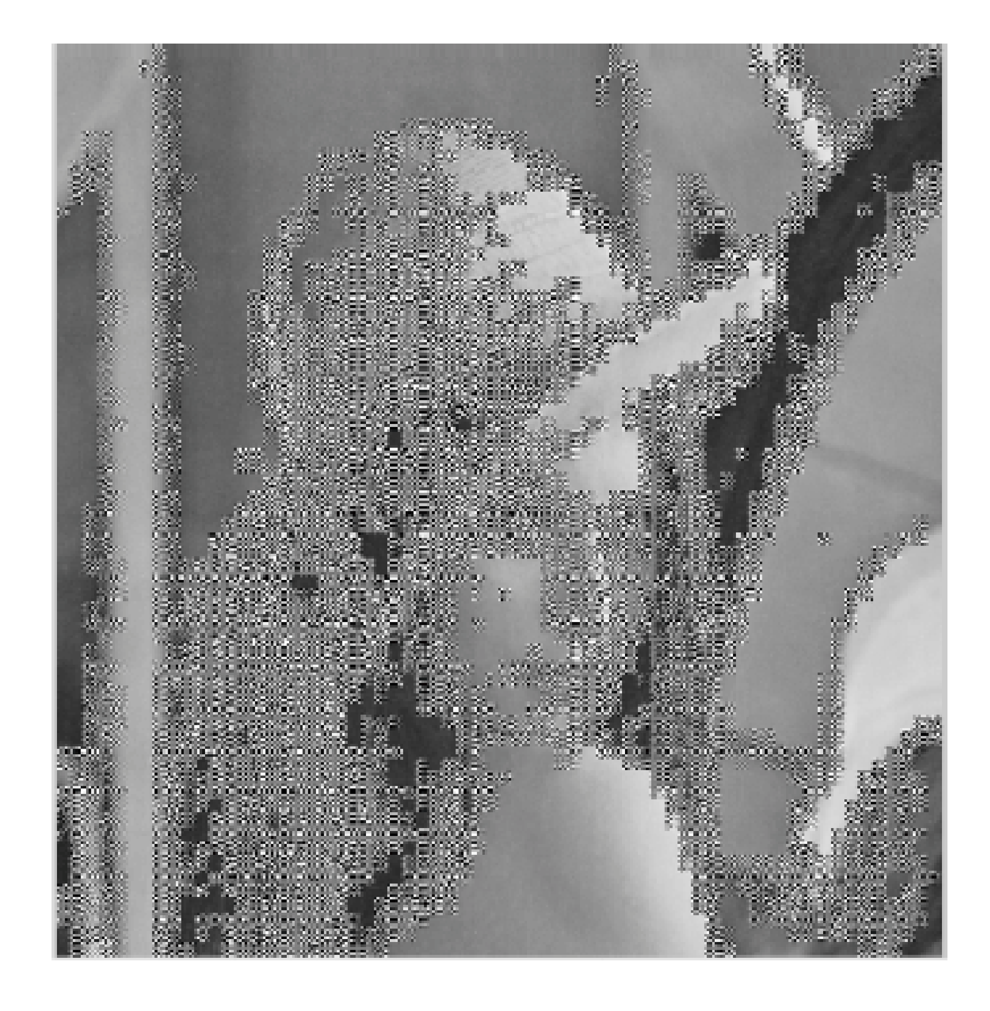
(b) Lanna上的模糊熵检测结果

图 7-8　利用模糊熵在图像上对特征的检测结果

图 7-9(a)、(b)是将水印的嵌入权值从全局统一放大若干倍，以反映水印在图像的特征区域的嵌入分布效果。水印的嵌入基于图像的 8×8 分块的 DCT 的中频系数。从两幅图像的水印化效果可以看出，水印的嵌入区域正是模糊熵显著的地方，而在平坦的区域，或者说图像像素变化不强烈的区域，则相对很少，甚至不可能嵌入到这些地方。并且，同样是这些区域，水印的明暗强度也是不同的，主要因为，在对水印嵌入强度处理中，使得水印的强度依赖于图像内容而变化，采用了图像局部统计特性的自适应算法。



(a) FEMA 对图像特征的提取效果



(b) 水印在图像中的分布

图 7-9　FEMA 对图像特征的提取效果及水印在图像中的分布

图 7-10 反映了全局调整因子 λ 和 PSNR 的关系，从图 7-10 中可以看出：λ 越大，PSNR 的值越小，水印对图像的改变越大。反之越小。图 7-10 也从另一个方面提供了一个从构造脆弱性水印到鲁棒性水印 PSNR 随调整因子变化的参考表。从试验中可以知

道，当 $\lambda \geqslant 0.4$ 时，图像已有明显的假象存在。当 $\lambda < 0.3$ 时，水印的加入是无感觉，再小的权值，可能就属于构造脆弱性水印的范围。这里以 Plane 为例，取 $\lambda = 0.3$（归一化像素值），这是通过实验观察保证水印容量最大和视觉不失真的最佳全局调整因子。

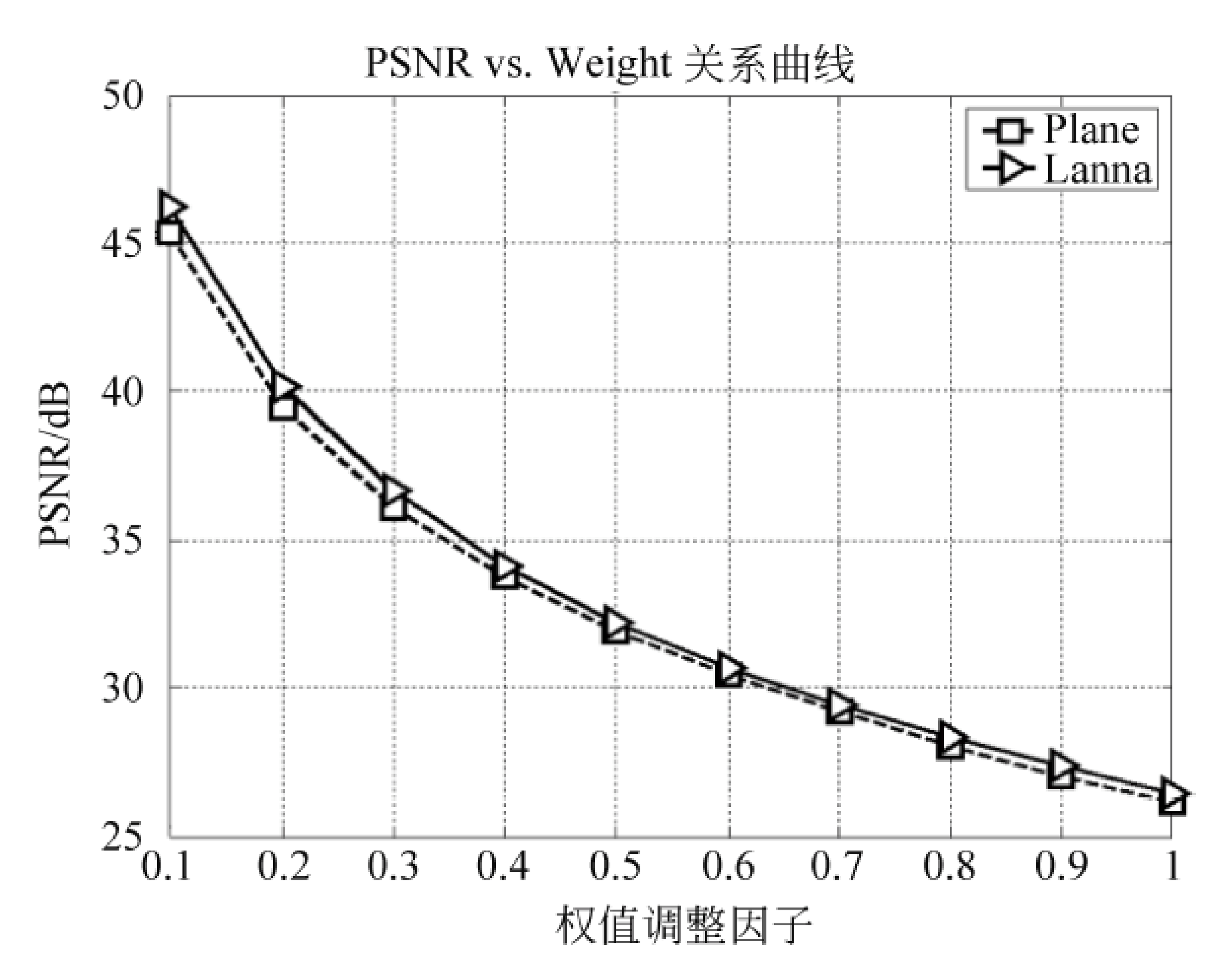


图 7-10 全局调整因子 λ 和 PSNR 的关系曲线

图 7-11 为水印化的 Plane 亮度图像，从中可以看出，这和原始的亮度图像没有任何感觉上的差异。



图 7-11 水印化的 Plane 亮度图像

图 7-12 是相关检测的结果。从水印化的图像中首先提取出特征系数，然后和参考的水印信息进行相关。这里是将二维置乱的参考水印首先转换成一维的参考序列。可以看出，当参考的序列和嵌入的水印相关时，会出现峰值，否则不会有峰值出现，或者相关性非常小。

利用 Kalman 滤波器对嵌入的水印信息进行提取时，将会出现误差。图 7-13 给出了在加噪的情况下，滤波器的检测误码率与信噪比之间的关系。

图 7-14 给出了 JPEG 压缩下 PSNR 的变化情况，试验中使用了 4 幅静态图像，分别

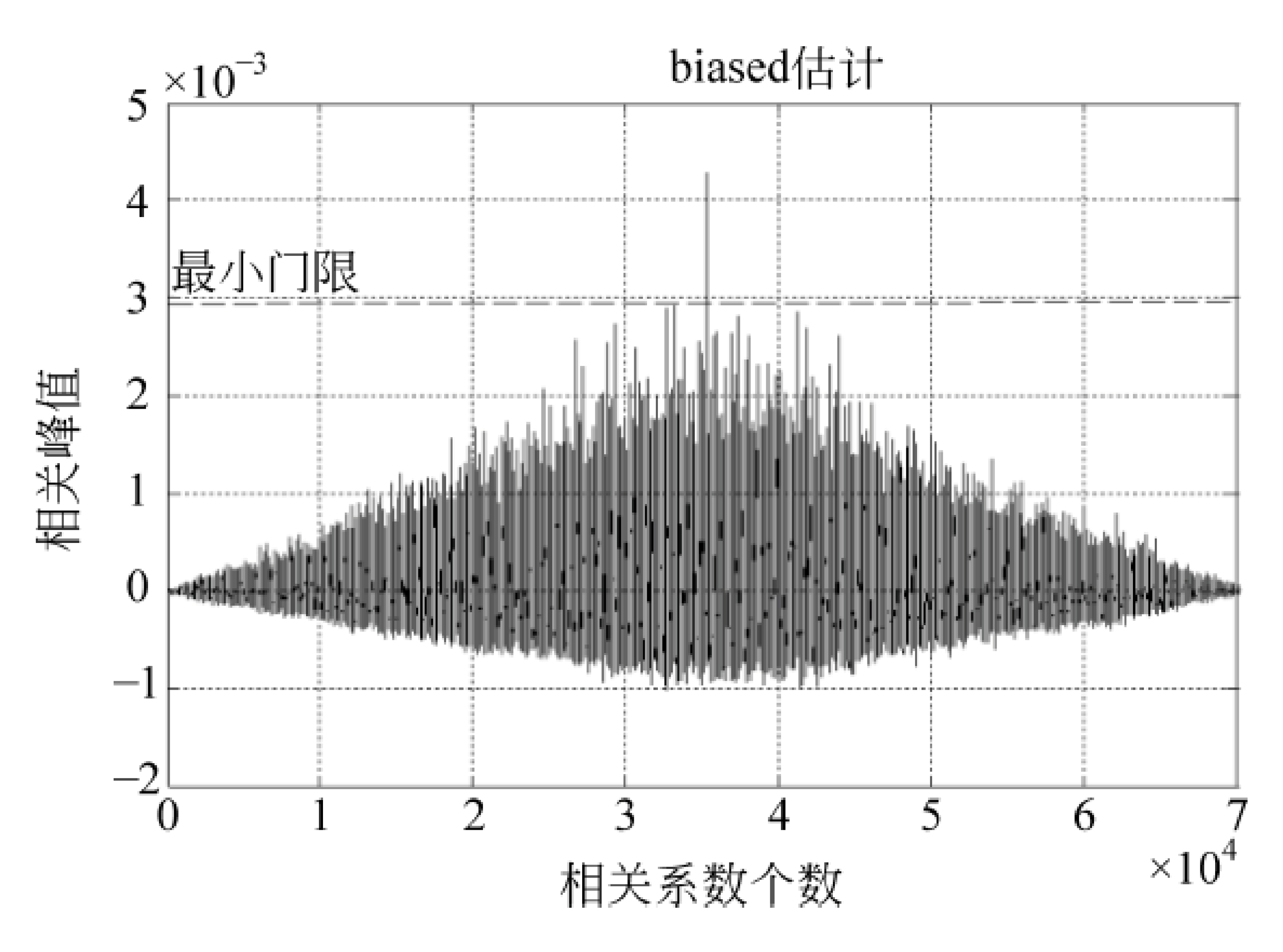


图 7-12　相关系数检测

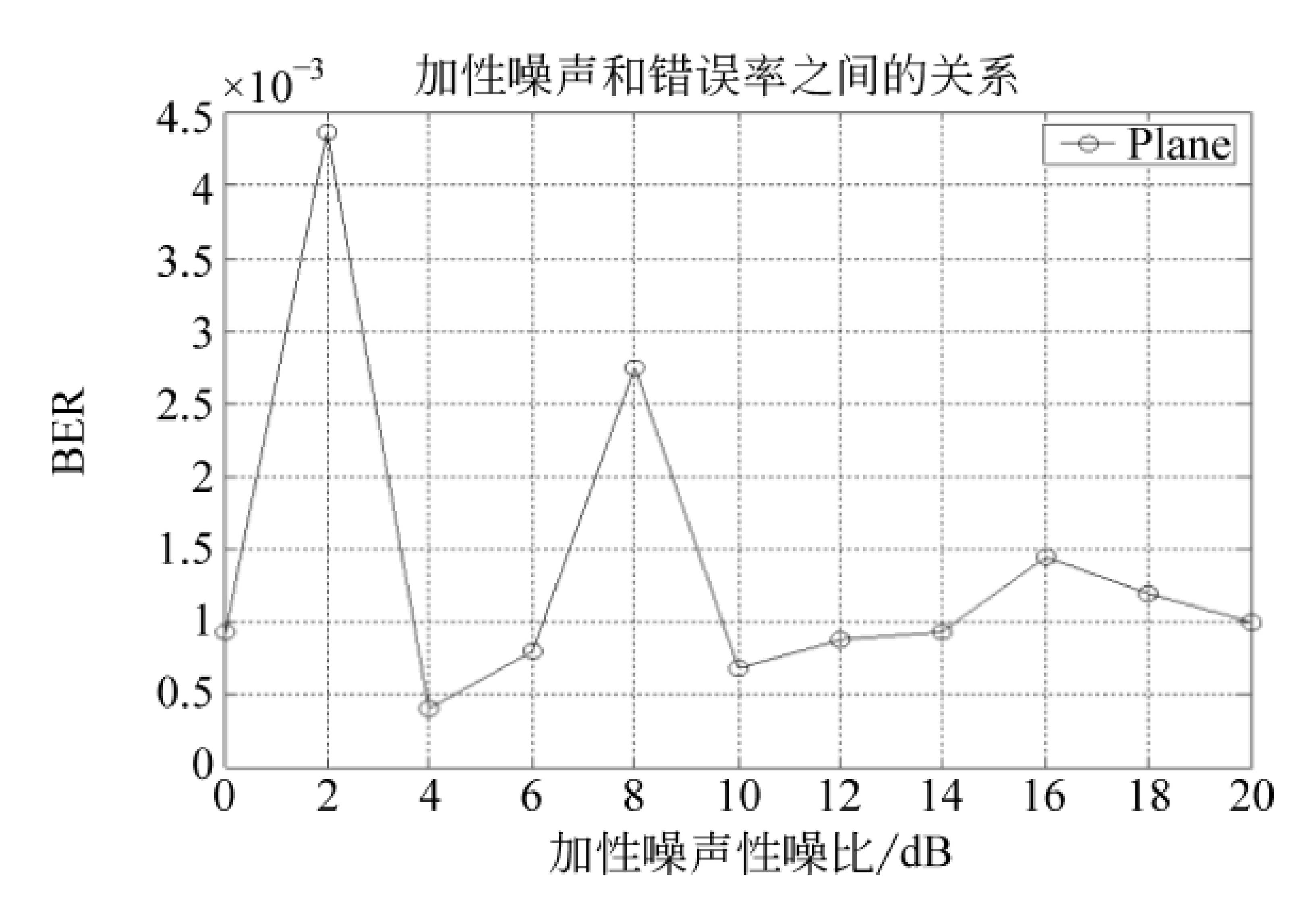


图 7-13　Kalman 滤波器在加噪下的误码率检测

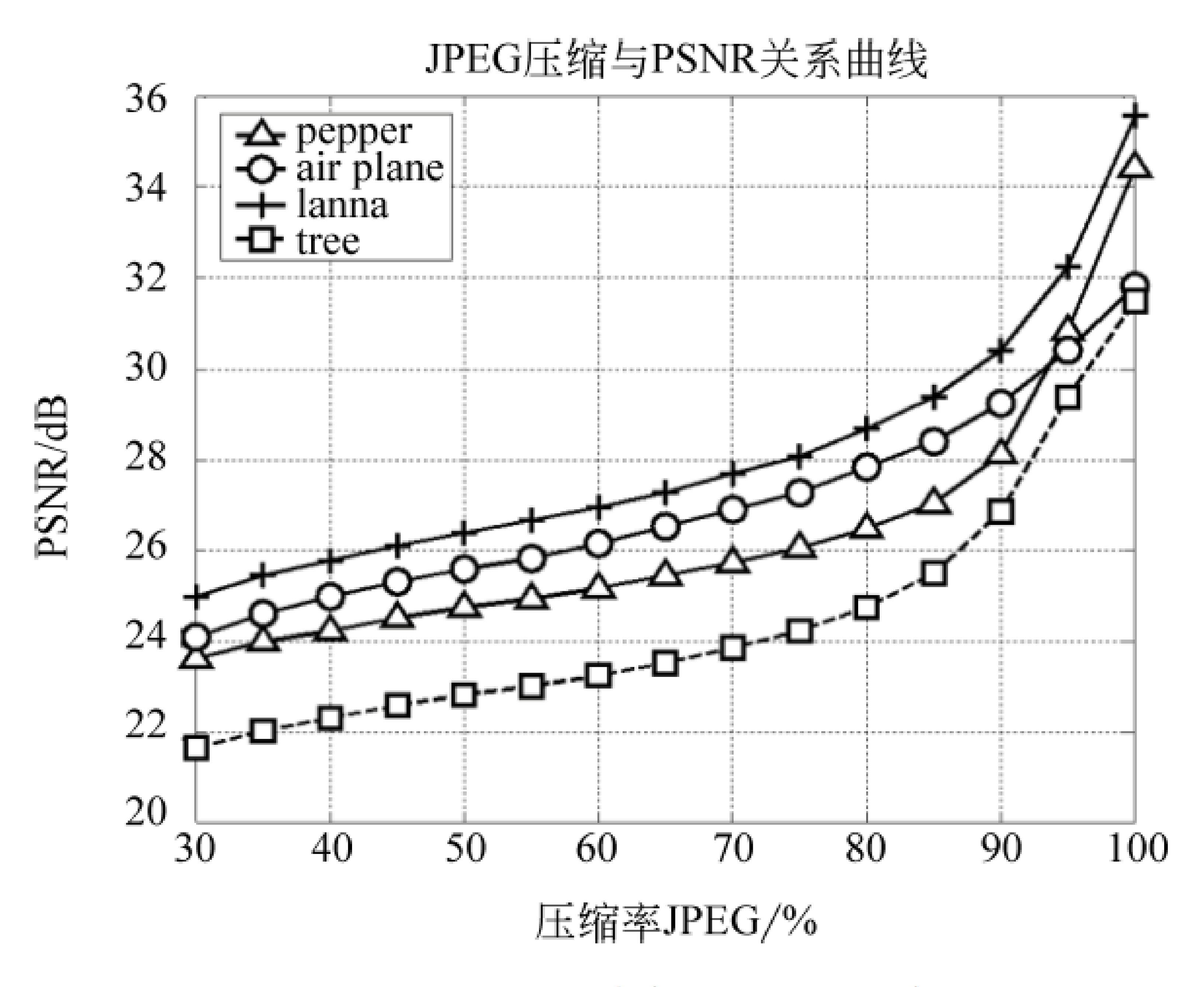


图 7-14　JPEG 压缩与 PSNR 的关系

是 Air plane、Lanna、Tree、Pepper。结果表明：在 JEPG 不同因子压缩下，所有图像的变化表现出的趋势大体一致。水印化的图像在 JPEG 因子下降到 35dB 时，开始出现明显的退化状态。

图 7-15 给出了中值滤波和 PSNR 的变化情况，试验中仍然使用了 4 幅静态图像。结果表明：在不同阶数滤波下，所有图像的变化表现出的趋势大体一致。水印化的图像在阶数到达 5 阶时，开始出现明显的退化状态。

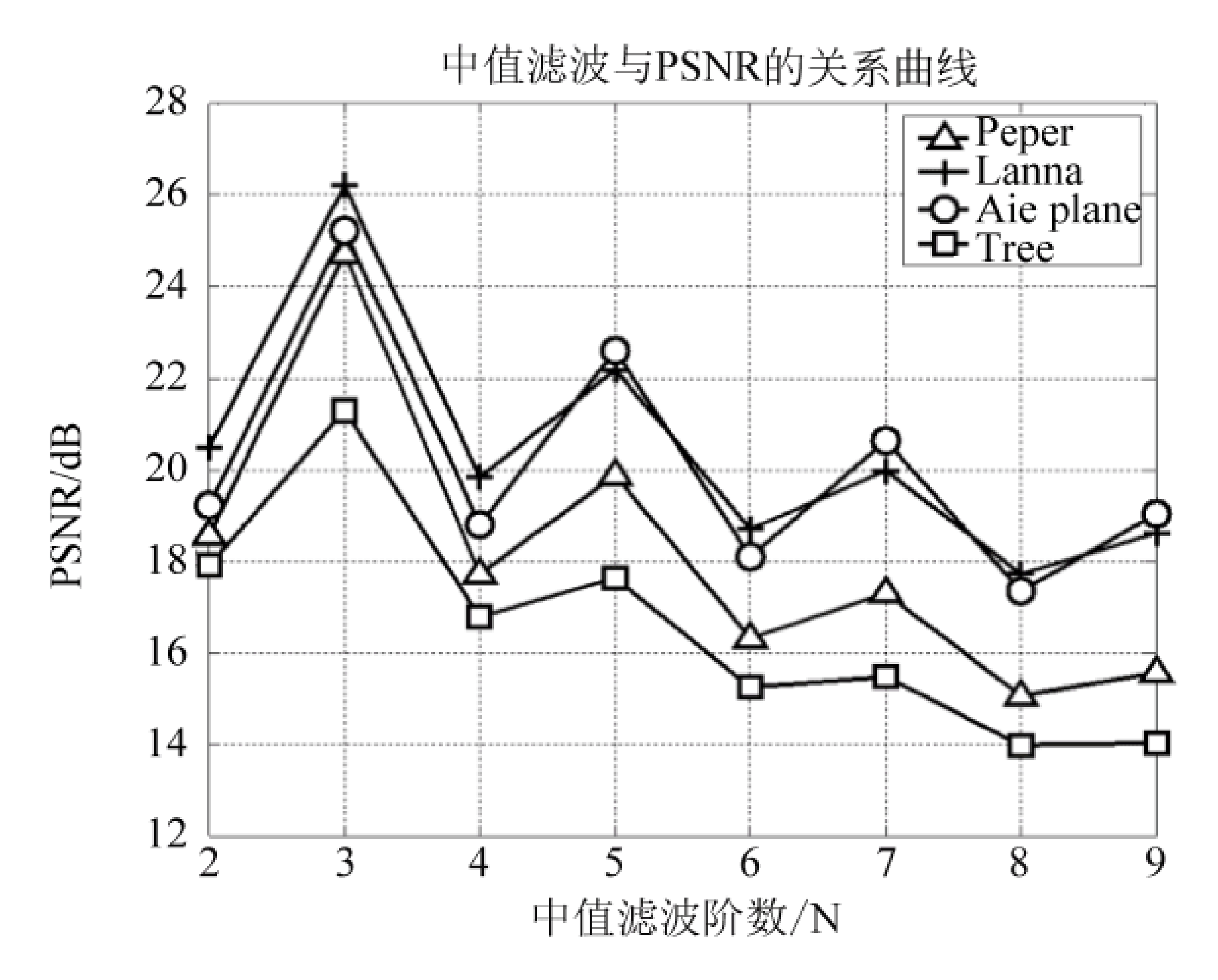


图 7-15　中值滤波与 PSNR 的关系

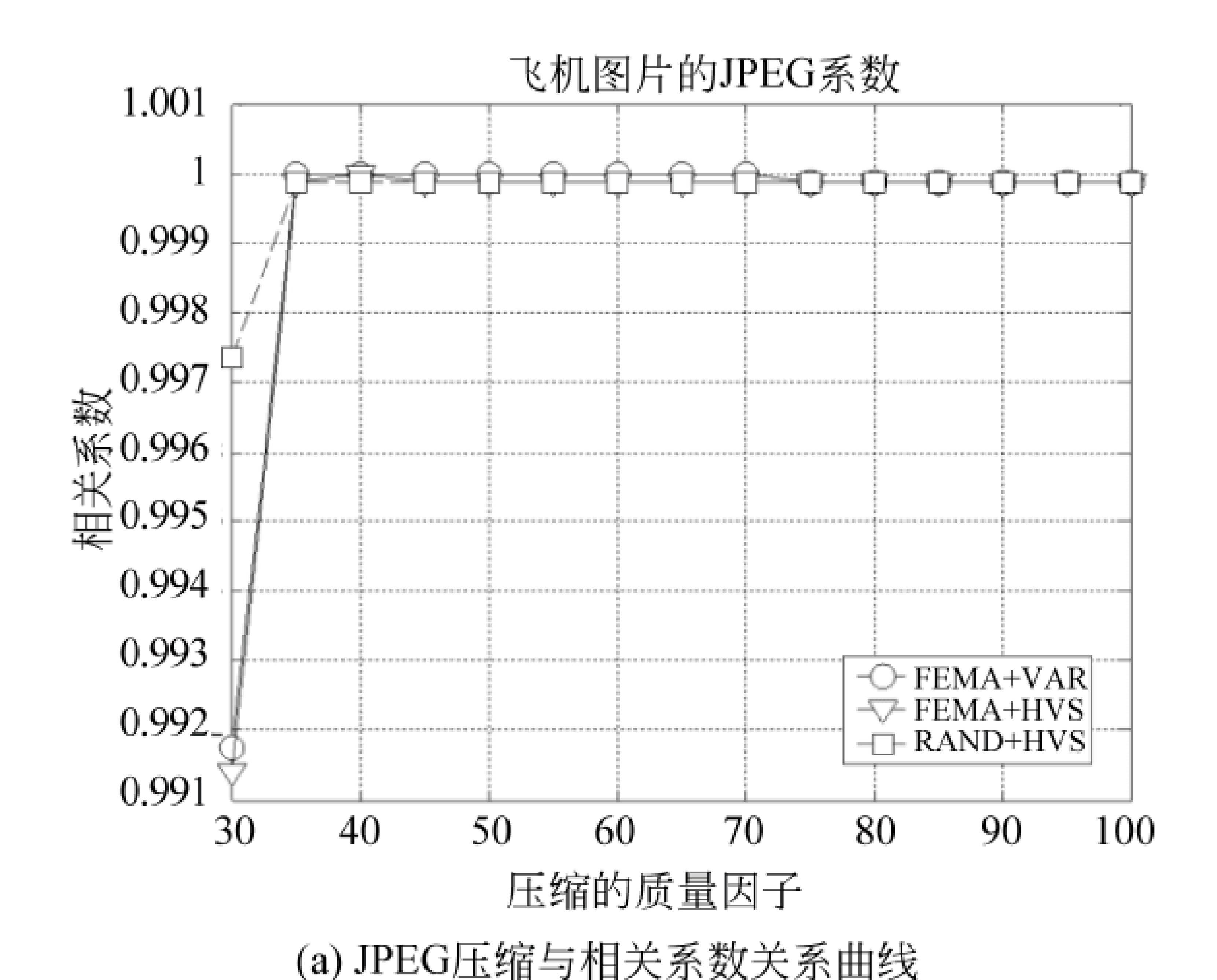
比较下面提出的水印方案和文献[144-145]中提出的基于 HVS 的水印方案，这里需要说明一下，我们只是采用了文献中的对水印权值的算法，并没有采用文献中的伪随机信号代替水印信息。本方案中，直接使用商标置乱形成水印信号，水印的检测采用 Kalman 滤波的方法，而不是采用原方案中的利用直方图的统计检测的方法。为了讨论方便，约定用 FEMA＋VAR 代表本方案；用 RAND＋HVS 代表原始的基于 HVS 模型的水印方案；用 FEMA＋HVS 代表将 FEMA 和 HVS 方案结合的水印方案。另外，商标的恢复统一使用提出的基于 FEMA＋VAR 的水印检测方案，宿主图像选择 Plane。

图 7-16(a)中给出了水印化图像在不同的 JPEG 压缩量化因子下的相关系数的检测结果。

首先，对水印化的图像进行 JPEG 压缩，可以看出水印化的图像在 JPEG 因子 35%以上时，3 种算法的检测结果基本趋于一致。在低的 JPEG 因子压缩情况下，FEMA＋VAR 明显好于其他两种方法。在压缩因子低于 30%时，水印化的图像已出现明显的失真，但利用 Kalman 预测以及恢复的商标有效。图 7-16(b)是 JPEG 因子为 45%时的商标恢复。

其次，对水印化的图像通过中值滤波器的滤波，如图 7-17 和图 7-18 所示。图 7-17(a)是不同阶数下中值滤波后的各个方法的检测结果，当滤波器阶数小于 3 时，3 种方法基本一致，阶数高于 3 时，FEMA＋VAR 方案的检测性能优于 HVS 方案，而 FEMA＋VAR 算法性能优于 RAND＋HVS 算法。图 7-17(b)是中值滤波阶数为 4 时的商标恢复。

最后，水印化图像经过了加噪声处理。图 7-18(a)是加高斯(Gaussian)噪声情况下，

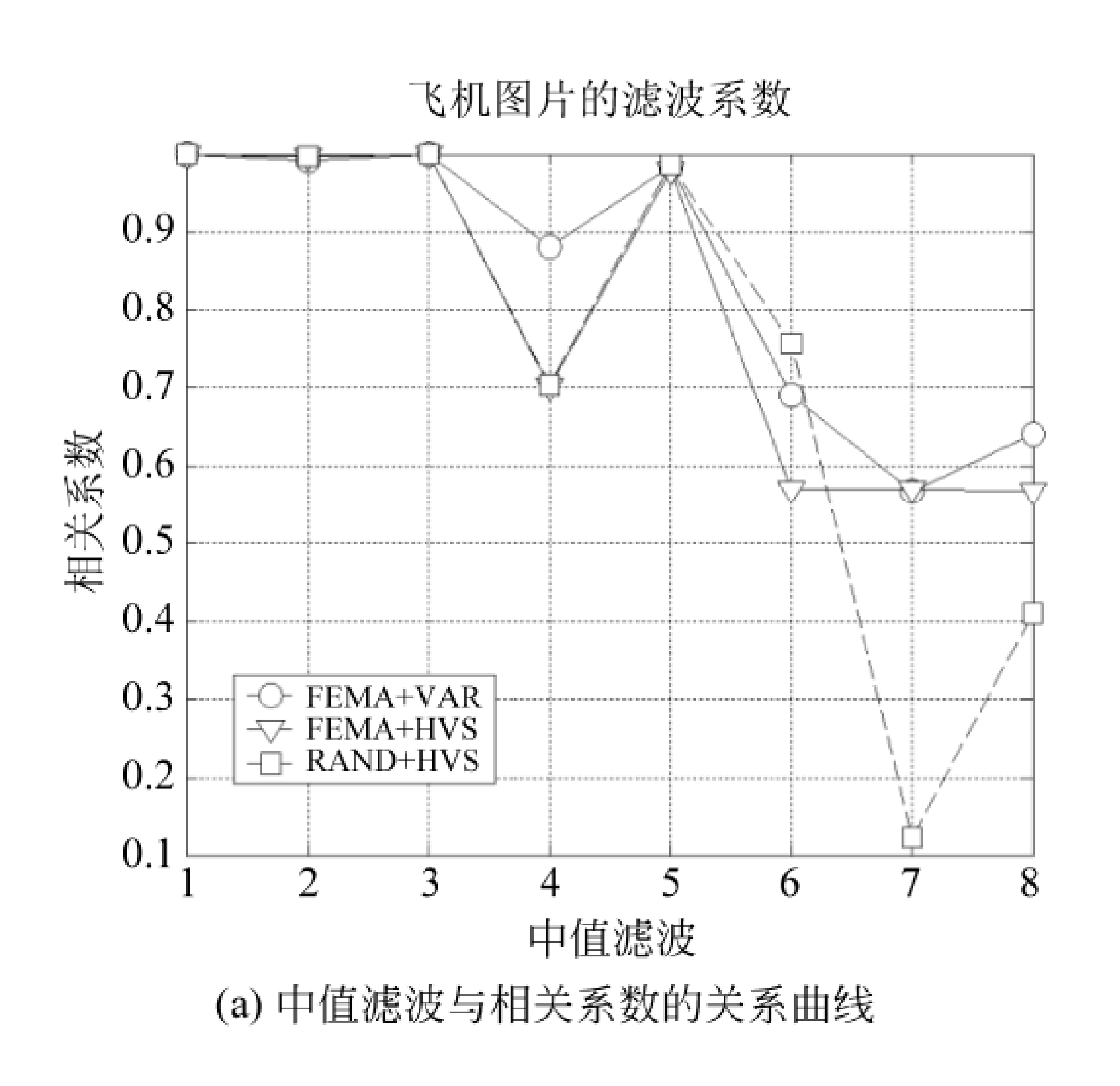


(a) JPEG压缩与相关系数关系曲线



(b) JPEG因子为45%时的商标恢复

图 7-16　JPEG 压缩下的检测结果



(a) 中值滤波与相关系数的关系曲线



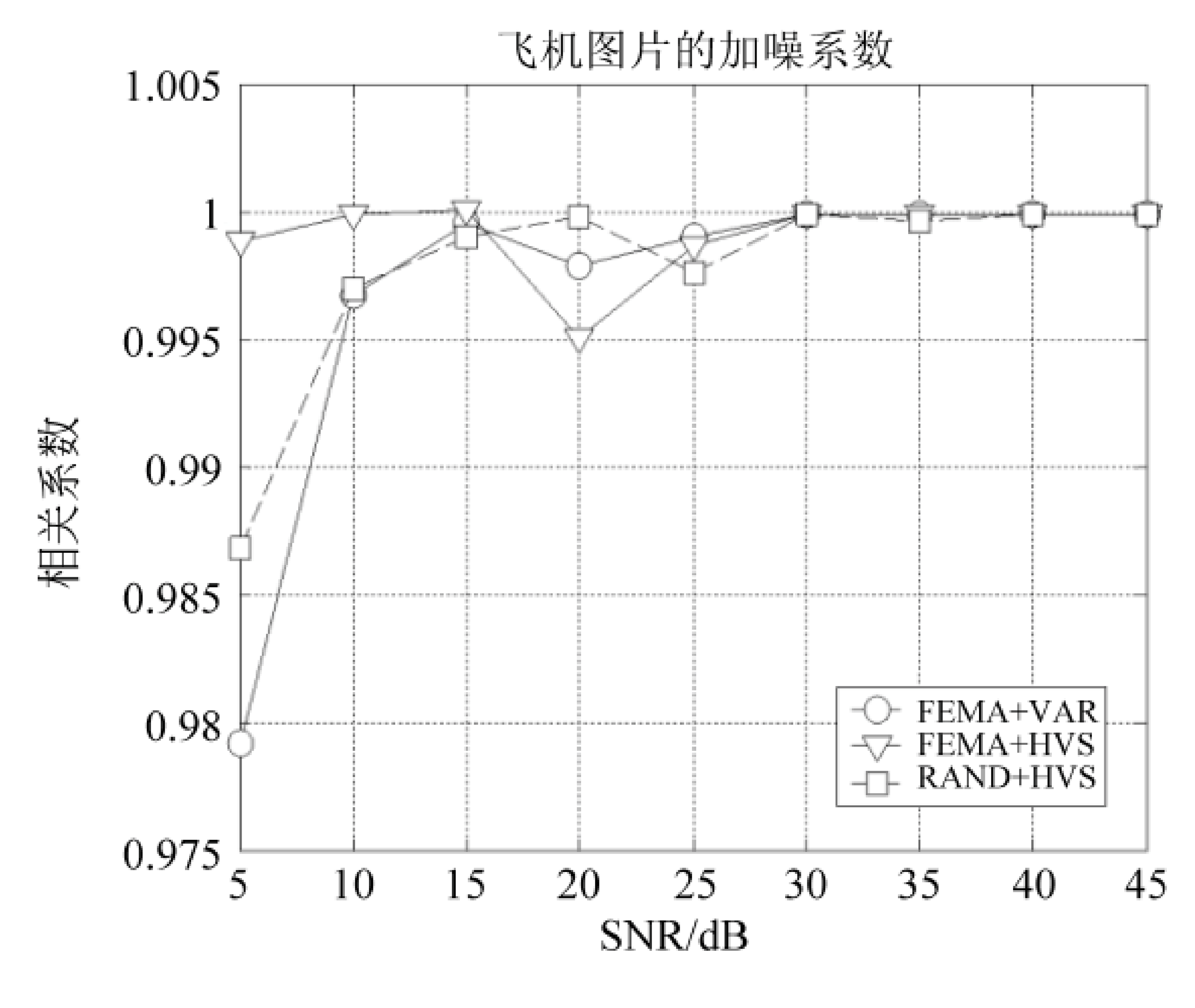
(b) 中值滤波阶数为4时的商标恢复

图 7-17　中值滤波下的性能检测

不同信噪比下的相关系数的检测情况。加入噪声后，滤波器的检测性能较其他信号处理要好，这可能是加入的噪声和水印信号不相关的缘故。在信噪比达到 30dB 左右时，水印化的图像有明显的视觉下降。而在 30dB 之下，FEMA＋HVS 方法的性能要优。图 7-18(b)为 SNR＝30dB 情况下商标的恢复。

对水印化图像的另一类重要的攻击类型是几何处理。下面对提出的水印方案以及文献[144-145]中的方案进行抗几何攻击检测。我们只对常见的几种攻击方法进行分析和比较，结果如下所述。

图 7-19(a)为剪裁情况下相关系数的变化。采用 FEMA＋HVS 方法的检测性能要优于其他两种方法。从原理上讲，FEMA＋HVS 方法采用的是一个空间域的“稀疏”映射。对水印化图像的剪裁，只能部分影响商标的回复信息。图 7-19(b)是在剪裁 40％情



(a) SNR与相关系数的关系曲线

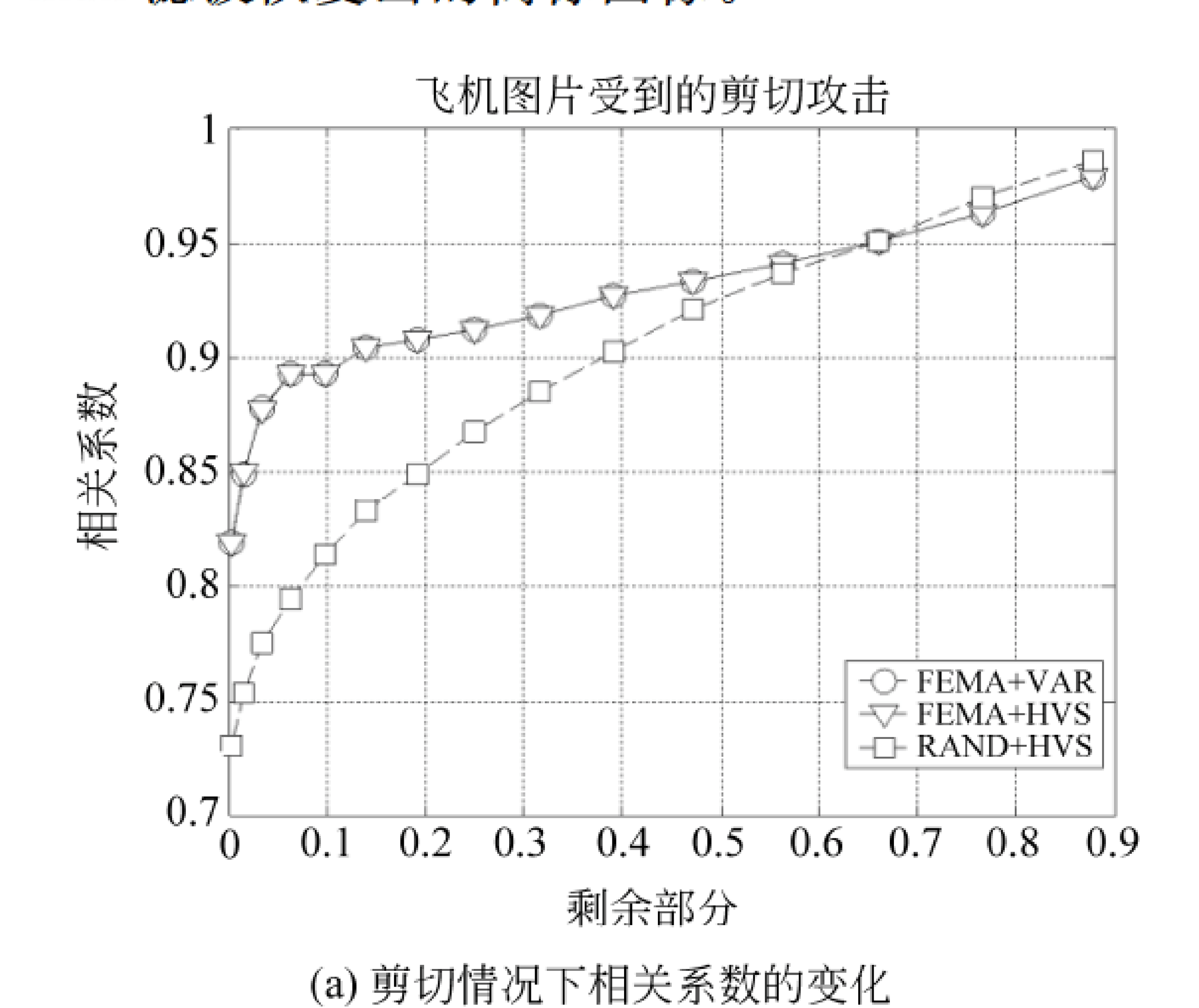


(b) SNR=30dB情况下商标的恢复

图 7-18　加噪情况下的检测结果

况下，Kalman 滤波恢复的商标图像。

图 7-19(a)为缩放情况下的相关系数的检测结果。采用 FEMA＋HVS 方法的检测性能要好于采用 FEMA＋VAR 方法。图 7-19(b)是在将水印化的图像剪切 40％时 Kalman 滤波恢复出的商标图像。



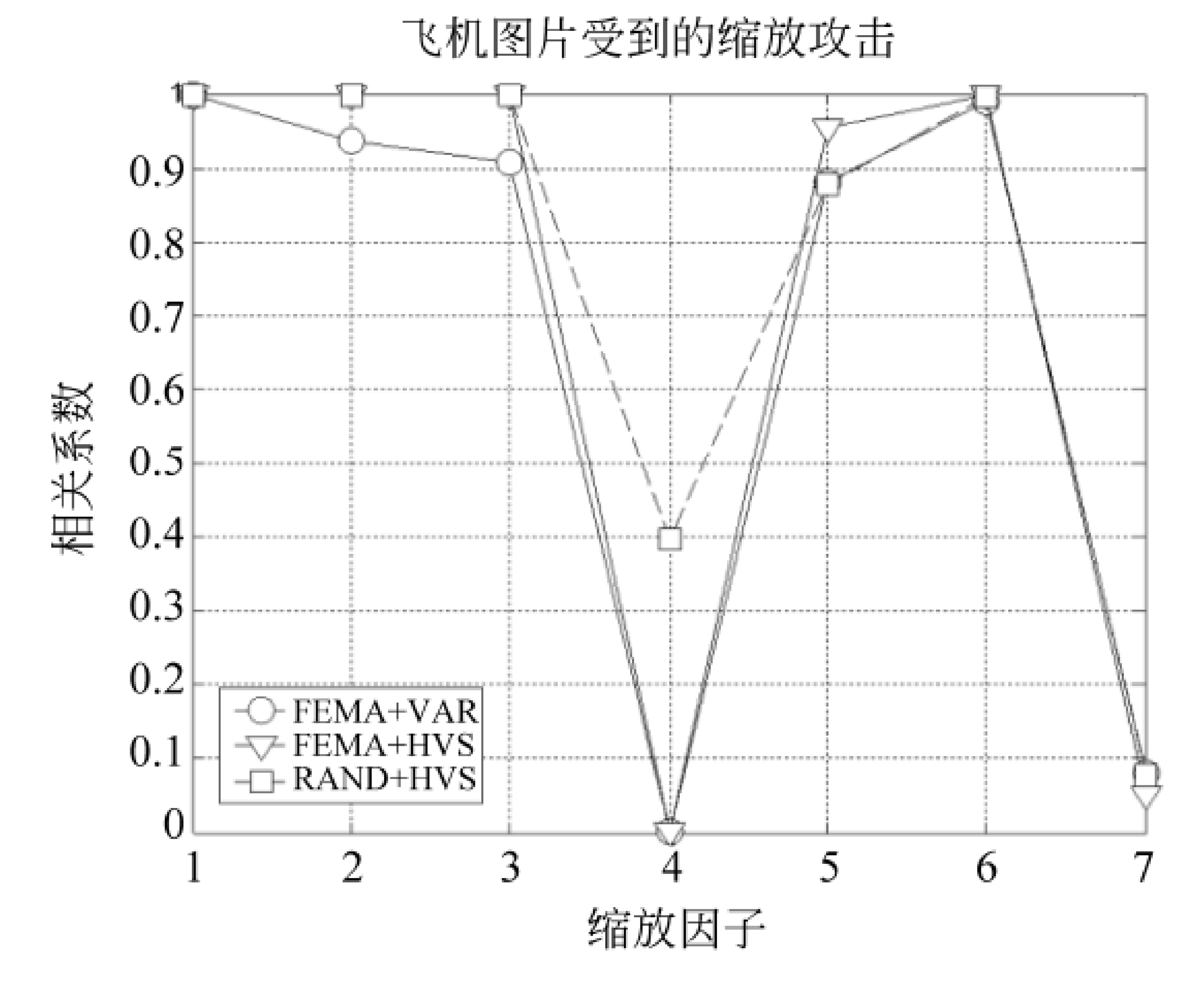
(a) 剪切情况下相关系数的变化



(b) 剪切40%时Kalman滤波恢复出的商标图像

图 7-19　水印抗剪切检测结果

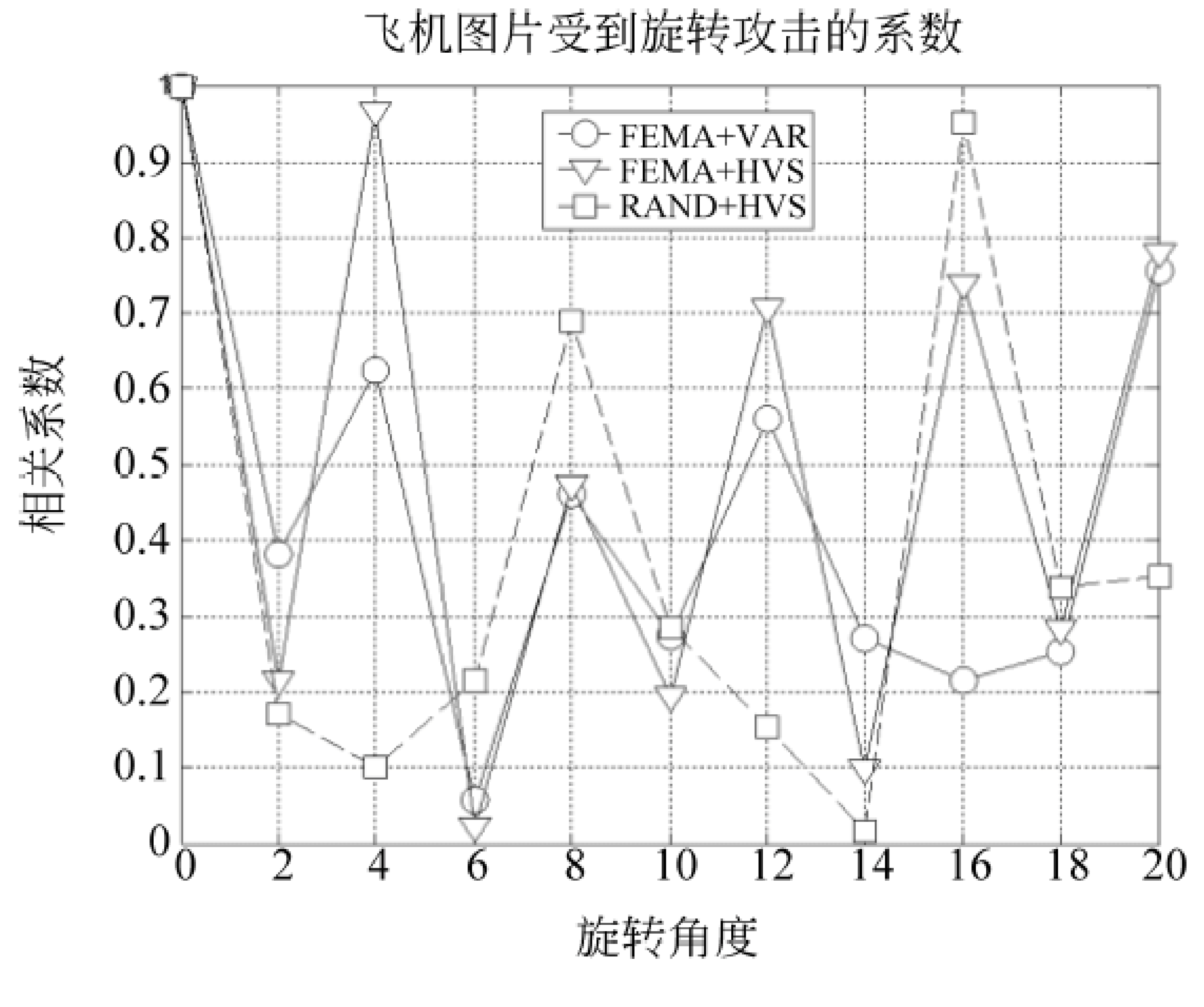
图 7-20 为水印抗缩放检测结果。图 7-21(a)为旋转情况下相关系数的变化。采用 FEMA＋HVS 方法的检测性能好于采用 RAND＋HVS 和 FEMA＋VAR 方法。图 7-21(b)是将水印化的图像旋转 15°时商标的恢复效果。



(a) 缩放情况下相关系数的变化

(b) 放大3倍时商标的恢复效果

图 7-20　水印抗缩放检测结果



(a) 旋转情况下相关系数的变化

(b) 旋转15°时商标的恢复效果

图 7-21　水印抗旋转检测结果

第 8 章 数字视频水印技术

在 MPEG-2/4 的视频压缩编码标准下，提出了基于视频序列动态特征的水印方案。利用图像模糊熵和帧图像的局部变化确定水印的嵌入权值，这种方案理论上不依赖 HVS 的方法。因此，构造的水印方案对基于 HVS 的 MPEG 压缩编码是鲁棒的。

8.1 视频压缩编码流程

如图 8-1 所示，MPEG-2 流具有分层的语法，从顶端到末端连续的结构中，Video 序列被分成多个图像组(GOPs)，一个 GOP 由多个单帧图像组成，而图像则由一个或几个片组成，每一片包含一个或多个宏块，由 4 个亮度块(Y)和两个色度块(U，V)组成，8 像素×8 像素的块是编码的基本单元。在 Y、U、V 块上进行 DCT，通过使用可变长编码进行编码，时间相关性通过从其他运动补偿的帧中预测而得到，预测的误差用来编码。MPEG-4 标准则建议基于对 Video 对象的描述，MPEG-4 认为每一场景由 Video 的对象组成，可通过对对象的运动、纹理和形状等特征描述。运动估计、纹理编码和在 MPEG-2 中对任意形状对象的自适应编码原理一样。

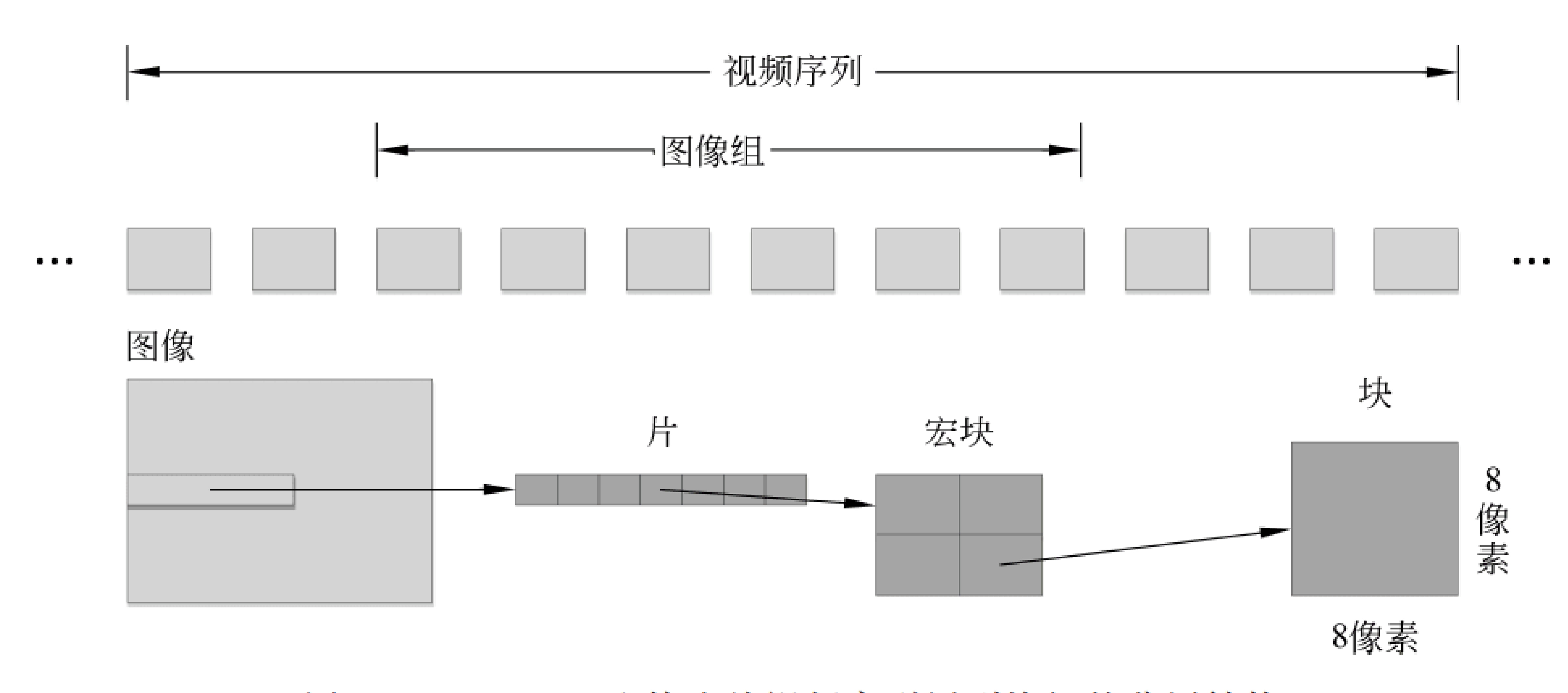


图 8-1　MPEG-2 比特流从视频序列层到块级的分层结构

对于静止图像，MPEG-4 采用零树小波算法(Zerotree Wavelet Algorithm)，以提高压缩比，同时还提供多达 11 级的空间分辨率和质量的可伸缩性。对于运动视频对象的编码，MPEG-4 采用了如图 8-2 所示的编码框图，以支持对象的编码。

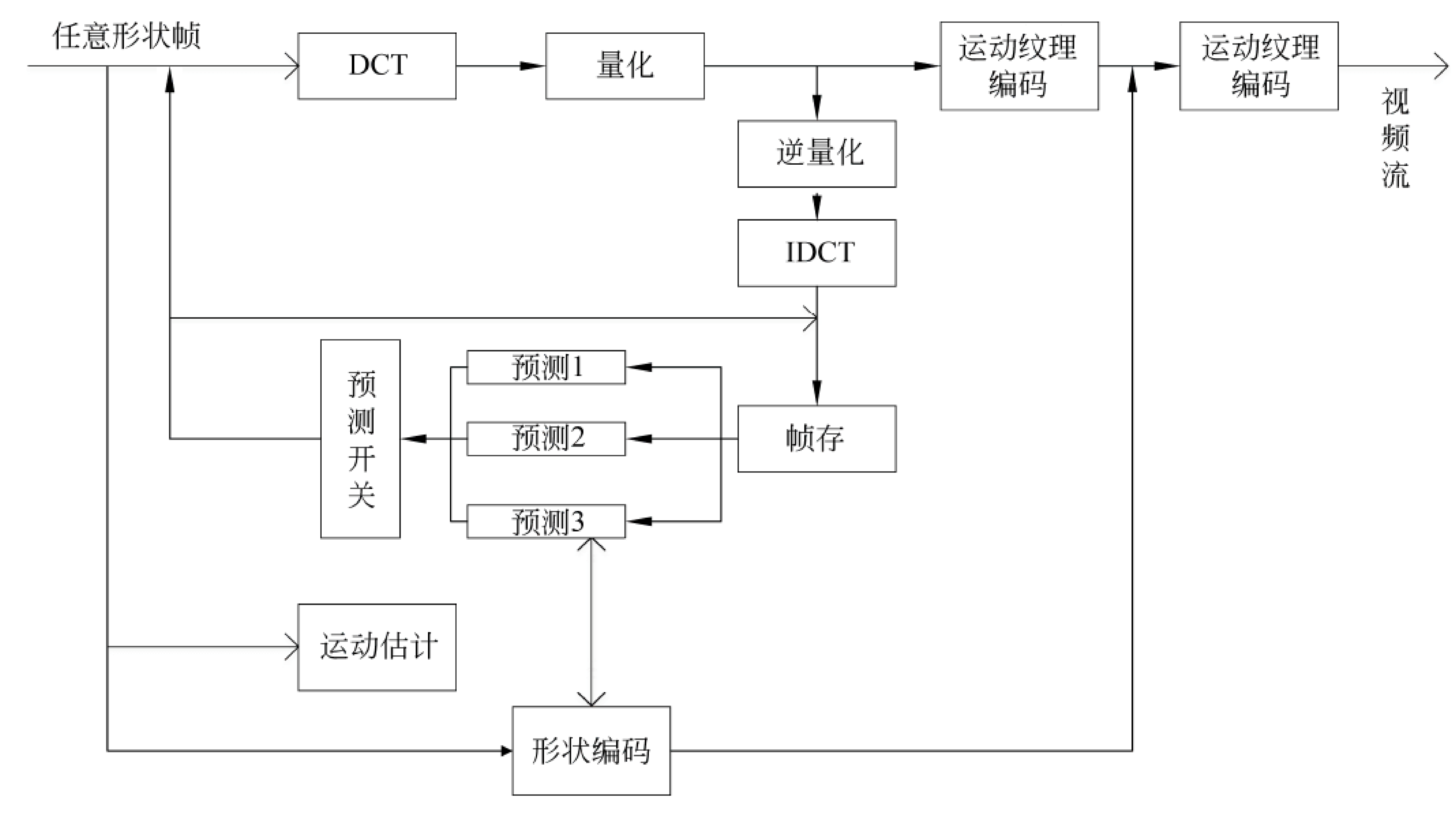


图 8-2　MPEG-4 编码框图

8.2 预测编码和运动估计

8.2.1 预测编码

预测编码分帧间预测编码和帧内预测编码。在预测编码时，传输的并不是像素的亮度抽样值本身，而是这个抽样值的预测值与实际值之间的差值。对这个预测误差进行量化后再编码，这种预测编码方式叫差分脉冲编码调制(Differential Pulse Code Modulation，DPCM)。

帧内编码：编码图像分块后直接进行 DCT，随后使用量化矩阵(Quantization Matrix)进行量化处理，以缩小数值的动态区域。由于量化后的数据是二维矩阵的形式，所以还需将二维数据扫描成一维数据，最后再进行可变长编码(VLC)，生成编码比特流送入缓冲器。

帧间编码：视频信号经过运动估计和运动补偿后，由运动矢量和参考帧生成当前帧的预测图像，而后将当前帧与预测图像的残差图像进行 DCT、量化、扫描和 VLC 编码，生成编码比特流送入缓冲器。

8.2.2 运动估计和运动补偿

由于相邻帧之间存在着时间冗余性和帧内空间冗余性，传送视频图像时，如果将每帧图像的所有像素全部传送，就会产生很多重复数据，也就是冗余信息，造成存储空间的浪费和传输速率的降低。如果只将物体的运动信息传送到接收端，接收端根据前一帧的图像信息和当前帧的运动信息更新出当前帧，这样传送的数据量就少了很多，而关键技术是

如何确定图像物体的运动信息，我们将这一过程称为运动估计（MotionEstimation，ME），表达方式称为运动矢量（Motion Vector，MV）。运动估计快匹配原理如图 8-3 所示。

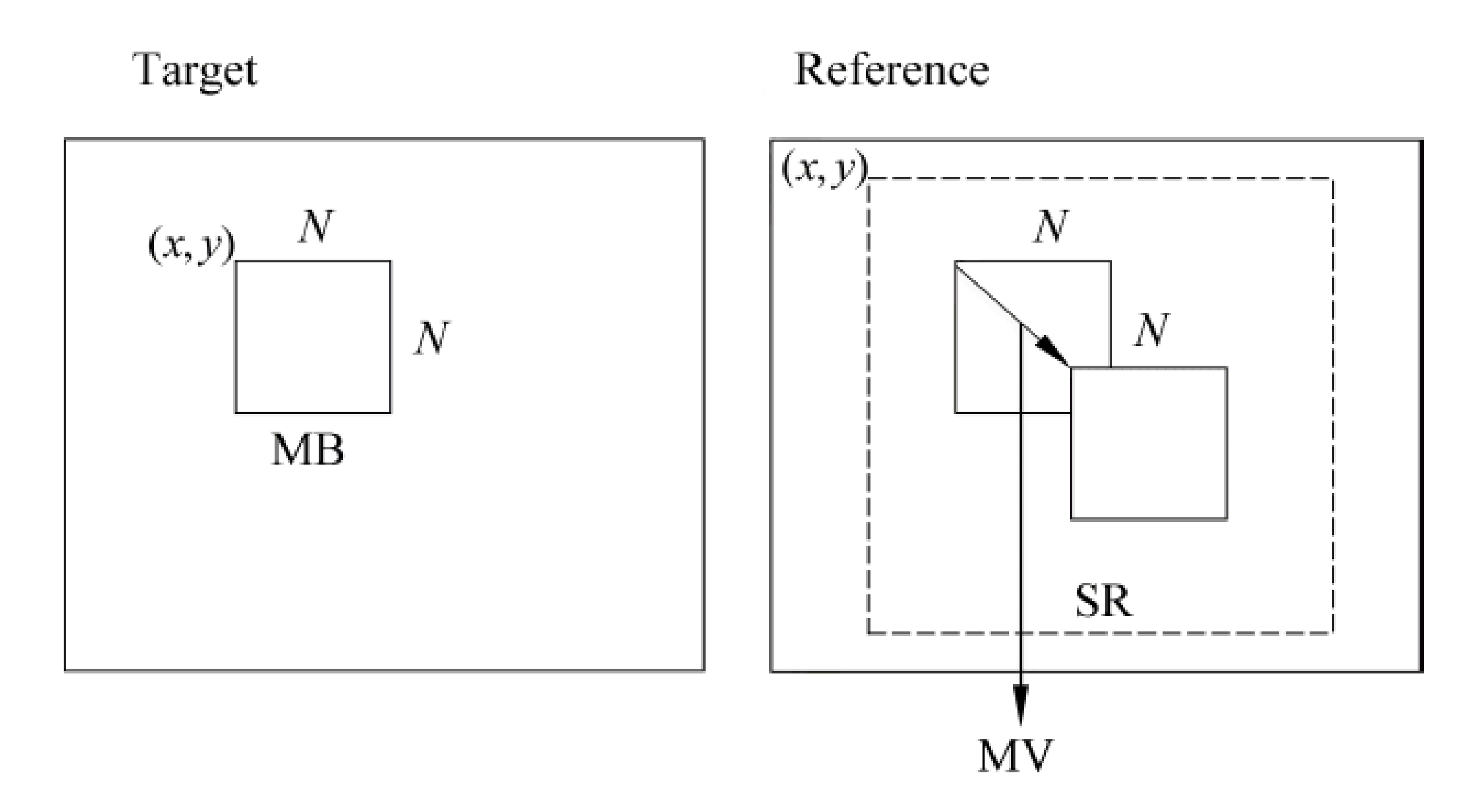


图 8-3　运动估计快匹配原理

类似于以前的视频编码标准，VOP 也有 3 种编码格式：I-VOP、P-VOP、B-VOP，表示 VOP 的运动补偿类型不同。

运动估计的过程是通过块匹配完成，块匹配运动估计研究包括块形状与大小、块匹配准则、搜索精度、搜索起点预测、搜索策略、算法评定指标等几个方面。目前，块形状与大小以及块匹配准则已经有了比较一致的选择；而搜索策略的选择最复杂，它决定了一个算法性能的好坏，因此，一直是块匹配运动估计研究的主要方向。

8.2.3　块的形状与大小

块匹配方法基于这样的假设：同一块内像素的运动是一致的。显然，这个假设具有一定的片面性，但选择合适的块形状与大小可在一定程度上消除这种片面性。一般来说，在块形状的选用上，正方形是比较自然的选择，这样既便于图像的划分，又有利于块匹配准则函数的计算。关于块的大小，显然划分得越小，残差就越小，但这使得编码效率降低了，块越小，越不能充分利用图像的空间相关性，所要编码的运动矢量也越多，如图 8-4 所示。

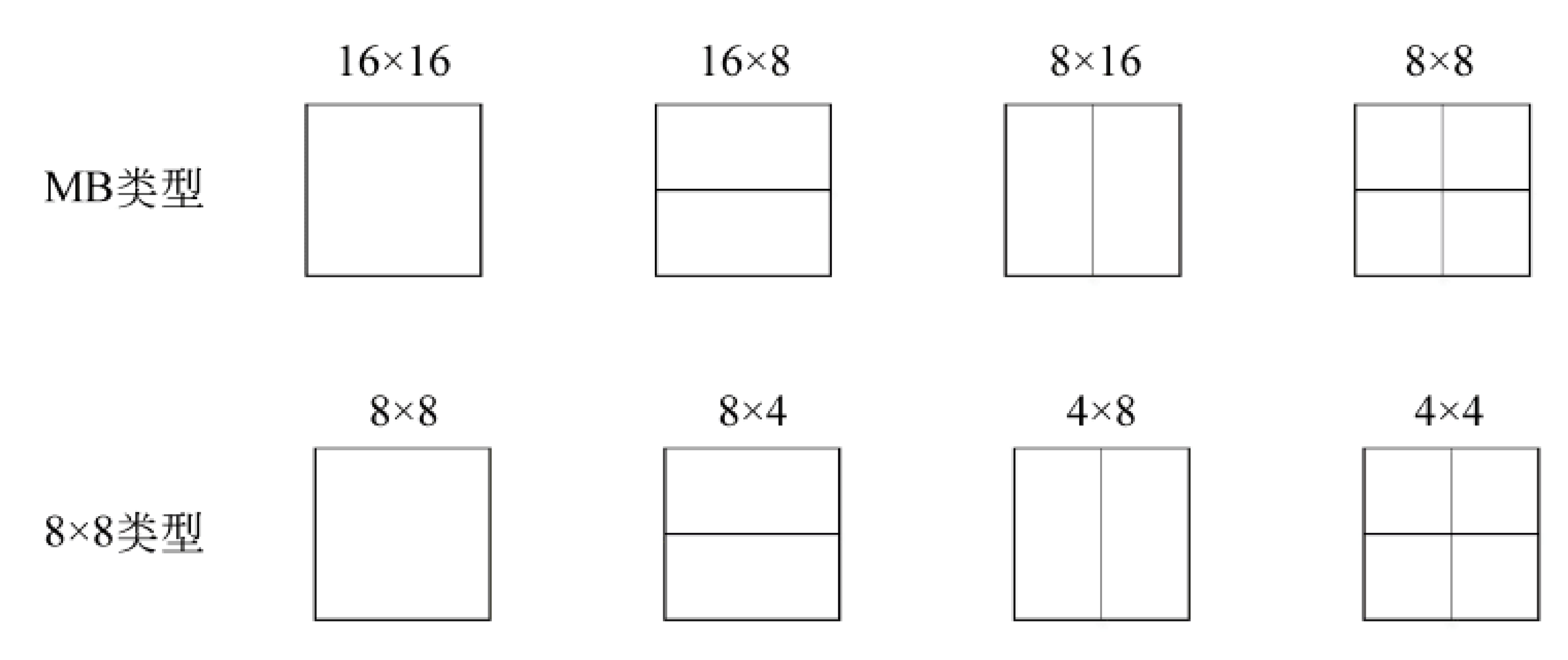


图 8-4　宏块及子宏块的分割

最新的视频压缩标准 H.264 中，宏块可划分成从 16×16 到 4×4 不同尺寸的子块，如图 8-4 所示。当选择比较大的块（如 16×16、16×8、8×16）进行编码时，意味着块类型

选择所用的比特数减少以及需要发送的运动矢量较少，但相应的运动补偿误差较大，因而需要编码的块残差数据较多；当采用较小的子块（如 4×4、4×8、8×4）进行编码时，一个宏块需要传送更多的运动矢量，同时子块类型选择所用的比特数增加，比特流中宏块头信息和参数信息占用的比特数大大增加，但是运动估计更加精确，运动补偿后的残差数据编码所用的比特数减少。因此，编码子块大小的选择对于压缩性能有比较大的影响。一般来说，大尺寸子块比较适于图像中灰度均匀区域，而小尺寸块适于有较多细节的区域。

8.2.4　块匹配准则

块匹配准则[167]是判断块相似程度的依据，因此匹配准则的好坏直接影响了运动估计的进度。另一方面，匹配运算复杂度、数据读取复杂度很大程度上取决于所采用的块匹配准则。因此，提高运动估计算法的速度有两种途径：一种是减少搜索匹配的点数；另外一种是降低块匹配准则的计算复杂度。常用的块匹配准则有以下几种。

（1）均方误差函数 MSE。

$$\mathrm{MSE}(\mathrm{d}x,\ \mathrm{d}y)=\frac{1}{XY}\sum_{x=1}^{X}\sum_{y=1}^{Y}[I(x,y,t)-I(x+\mathrm{d}x,y+\mathrm{d}y,t-\tau)]^2 \tag{8-1}$$

式(8-1)是计算相邻帧对应矩形区域($X\times Y$)内的最小均方误差，以 MSE 值最小为最优匹配点，其中 $-p\leqslant \mathrm{d}x,\ \mathrm{d}y\leqslant p$，$p$ 为允许的最大位移，X、Y 为宏块尺寸，匹配函数值为块失真度(BDM)，$I(x,\ y,\ t)$表示 t 时刻点上$(x,\ y)$的像素值。这是一种非线性测量，能较好地跟踪图像的协方差模型。

（2）绝对平均误差函数 MAD。

$$\mathrm{MAD}(\mathrm{d}x,\ \mathrm{d}y)=\frac{1}{XY}\sum_{x=1}^{X}\sum_{y=1}^{Y}\left|I(x,y,t)-I(x+\mathrm{d}x,y+\mathrm{d}y,t-\tau)\right| \tag{8-2}$$

式(8-2)是最简单的匹配准则函数，用它计算相邻帧间的绝对平均误差，以 MAD 值最小为最优匹配点。

（3）归一化相关函数 NCCF。

$$\mathrm{NCCF}(\mathrm{d}x,\ \mathrm{d}y)=\frac{\sum_{x=1}^{X}\sum_{y=1}^{Y}\left|I(x,y,t)-I(x+\mathrm{d}x,y+\mathrm{d}y,t-\tau)\right|}{\left[\sum_{x=1}^{X}\sum_{y=1}^{Y}I^2(x,y,t)\right]^{\frac{1}{2}}\left[\sum_{x=1}^{X}\sum_{y=1}^{Y}I^2(x,y,t-\tau)\right]^{\frac{1}{2}}} \tag{8-3}$$

以 NCCF 值最大为最小函数 MME

$$\mathrm{MME}(\mathrm{d}x,\ \mathrm{d}y)=\max\left|I(x,y,t)-I(x+\mathrm{d}x,y+\mathrm{d}y,t-\tau)\right| \tag{8-4}$$

绝对误差和 SAD

$$\mathrm{SAD}(\mathrm{d}x,\ \mathrm{d}y)=\sum_{x=1}^{X}\sum_{y=1}^{Y}\left|I(x,y,t)-I(x+\mathrm{d}x,y+\mathrm{d}y,t-\tau)\right| \tag{8-5}$$

实验表明，MSE 匹配函数运动估计的精度最高，但其众多的乘方运算在 VLSI 实现比较困难，MAD 匹配函数略差，但其相对简单的运算易于在 VLSI 中实现；MME 匹配函数过于简单，没有充分利用匹配块所包含的特征信息，使运动估计的精度大大降低。相对而言，只有 MAD 准则函数比较实用，一度得到广泛的应用。

SAD准则出现后，迅速取代MAD被各种运动估计算法采用，因为它与MAD的匹配效果等价，使得计算量大大降低。这是因为：一方面，它不需乘法运算，实现简单方便；另一方面，在计算SAD的过程中，当发现块的部分SAD已经大于当前SAD时，可以中途退出，从而大大减小计算量。

8.2.5 像素搜索精度

在视频序列中，帧与帧之间的真正位移并非总是像素尺寸的整数倍。如果可以获得亚像素精度的运动矢量，则可以提高运动预测的精度。对于1/2、1/4像素精度预测，由于在参考帧中不存在这些位置的像素值，因此需要采用周围的像素差值计算。

8.2.6 初始搜索点的选择

(1) 直接选择参考帧的(0,0)位置。这种方法简单，但容易陷入局部最优点。如果采用的算法初始步长太大，而原点又不是最优点，又可能使快速搜索跳出原点周围可能比较大的区域而去搜索远距离的点，导致搜索方向的不确定性，故有可能陷入局部最优。

(2) 选择预测的起点。相邻块之间具有很强的相关性，以预测点作为搜索起点。大量的实验证明预测点更靠近最佳匹配点，使得搜索次数减少。序列图像的运动矢量在空间和时间上具有很强的相关性，特别使属于同一对象的块运动保持一致的可能性更大，这时若取相邻块的运动矢量预测搜索起点，会使得中心偏移更加集中。

8.3 搜索策略

搜索策略[168]选择得恰当与否对运动估计的准确性和算法效率都有很大的影响。

8.3.1 全搜索法

全搜索(Full Search，FS)法是对搜索范围内所有可能的候选位置计算SAD(i,j)的值，从中找出最小SAD，其对应的偏移量即所求运动矢量。此算法虽简单、可靠，找到的必为搜索范围内的全局最优点，但计算量大，占据了整个编码大约80%的计算量，很难用于实时应用，如图8-5所示。

8.3.2 三步搜索法

三步搜索(TSS)法得名于它原来的三步搜索(搜索窗口为±7时)，当搜索窗口变大时，步数就不止三步了。它是一种由粗到精的搜索算法，快速而且高效。三步搜索算法实现简单，由于收敛迅速，很快就能结束搜索过程。TSS在视频会议和可视电话中应用极多，但是搜索过于粗糙，由于初始步长为2^{N-1}，因此很容易一开始就跳出最优匹配可能性比较大的区域，到偏离最优点很远的地方搜索而陷入局部最优。但三步搜索算法缺少对现实视频序列的中心偏置特性的考虑，新三步搜索算法(New Three-Step Search，NTSS)在这方面做了改进，从而获得比三步搜索算法更好的性能，如图8-6所示。

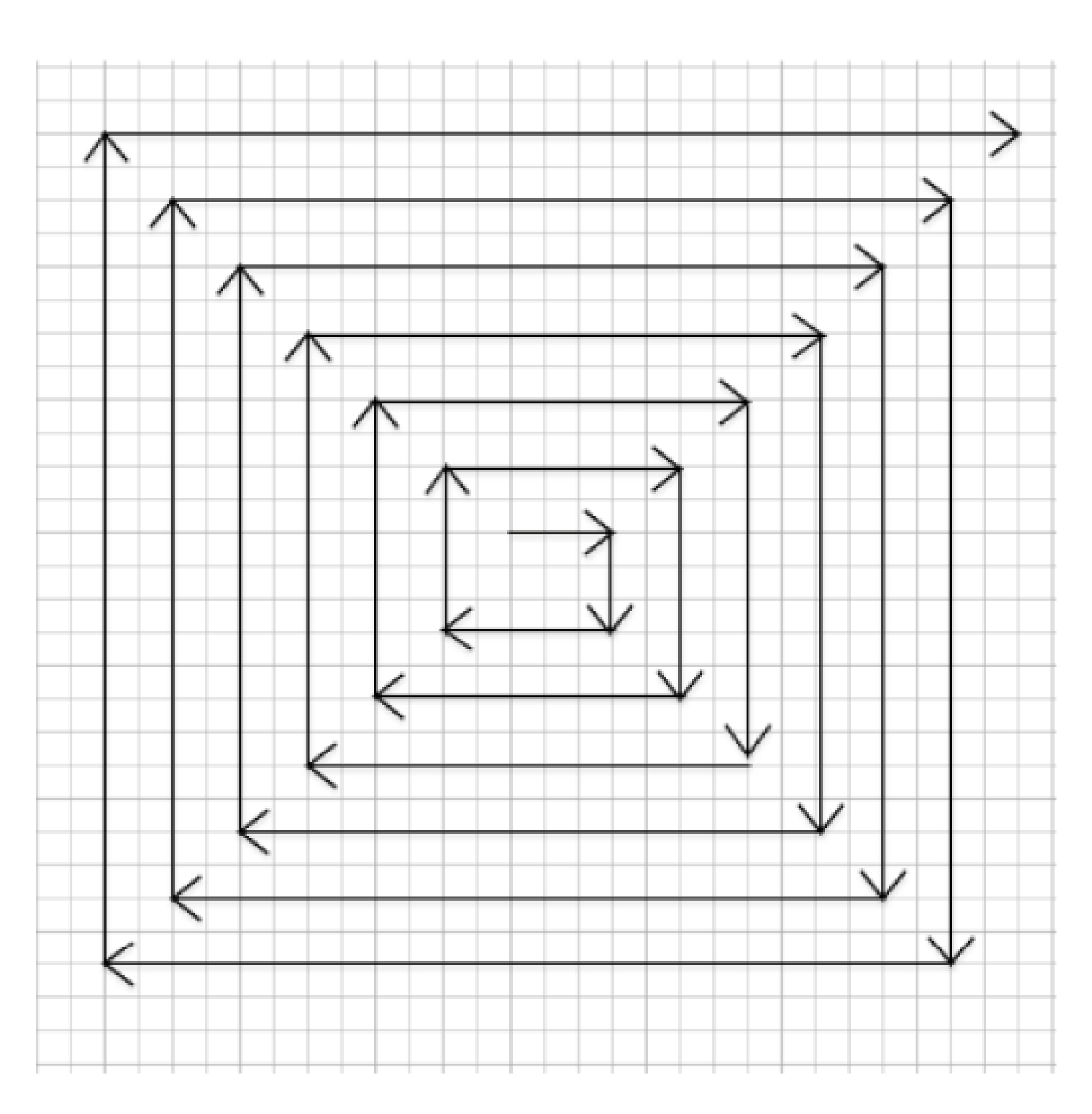


图 8-5　全搜索算法示意图

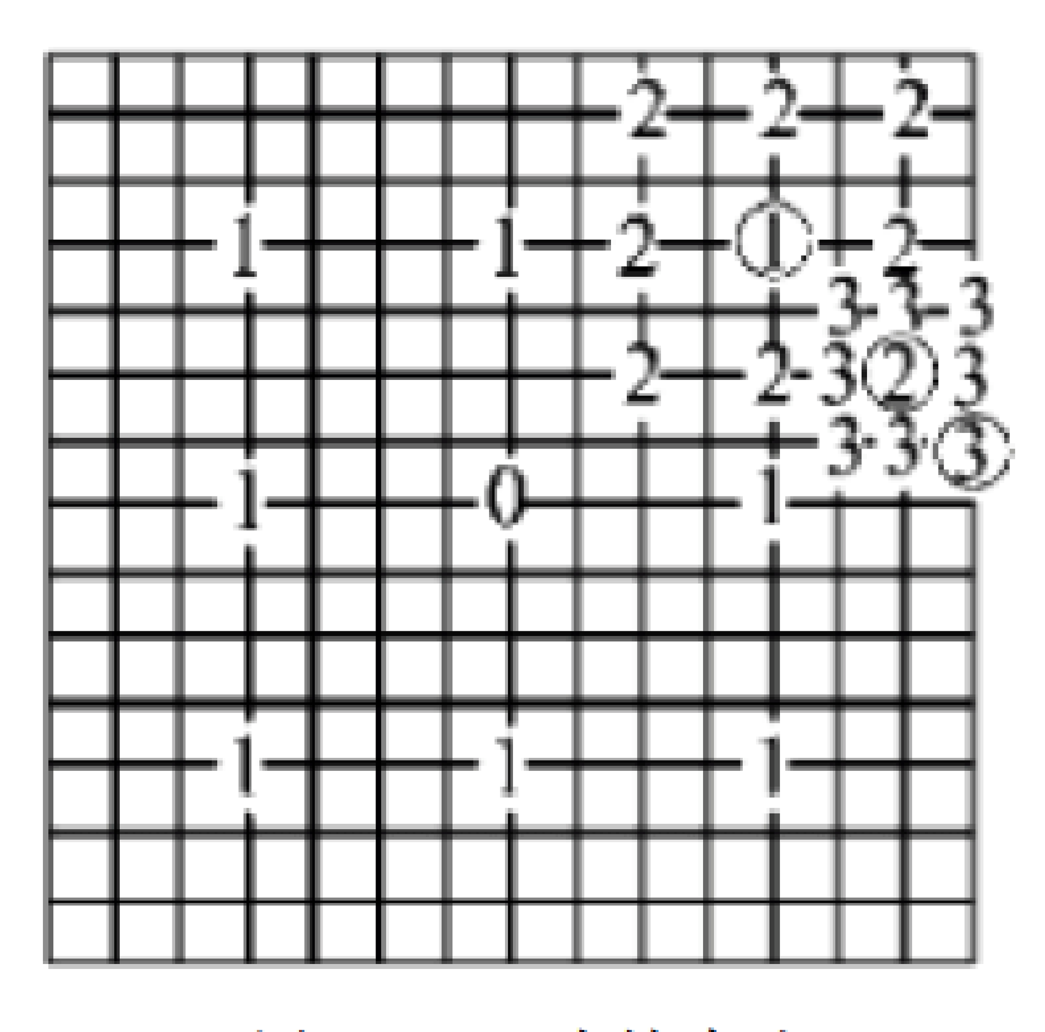


图 8-6　三步搜索法

8.3.3　新三步搜索法

新三步搜索法与三步搜索法的不同之处在于：①改进了原有三步搜索法第一步中搜索固定 9 个点的方法，采用了基于中心偏置的新搜索模式；②对静态子块或者准静态子块的搜索引入了中途停止的功能。通过对经典视频序列的实验得出，在一系列连续的视频帧中，大部分的块都有静态性和缓慢运动特性，因此在新三步搜索法的第一步运算时，对搜索窗口中心相邻的 8 个点也同时做了匹配运算，这样对慢速运动的物体可以很快地找到与之匹配的块。新三步搜索法利用运动矢量的中心偏置特性，采用了具有中心倾向的搜索点模式，并使用中止判别技术减少搜索次数，如图 8-7 所示。

由于宏块的中心偏置特性在现实中普遍存在，通常情况下只匹配很少的点即可完成搜索。中心倾向的搜索点模式不仅提高了匹配速度，而且减少了嵌入局部极小的可能性；而采用中止判别技术则大大降低了搜索复杂度，提高了搜索效率。

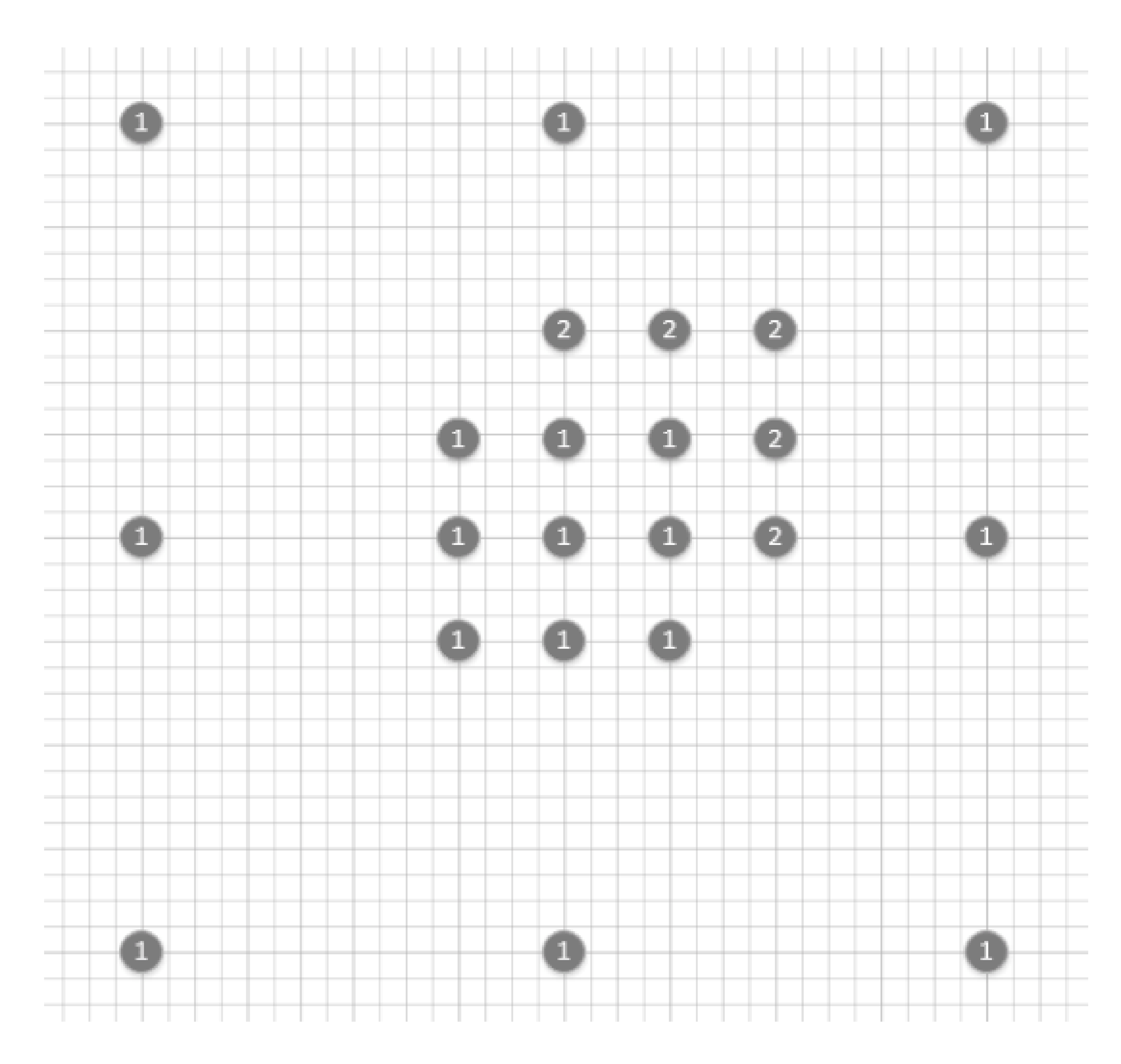


图 8-7　新三步搜索法示意图

8.3.4　四步搜索法

现实世界的物体既会有小范围的移动，也会有大范围的运动，因此，在考虑块匹配算法时，既要照顾块的中心偏置特性，也要兼顾块的大范围运动特性。四步搜索(Four-Step Search，FSS)法在两种情况下都能得到较好的特性。四步搜索法首先用 5×5 的搜索窗口，每一步将搜索窗口的中心移向最小快失真(MBD)点处，且后两步搜索窗的大小依赖于最小块失真点的位置，如图 8-8 所示。

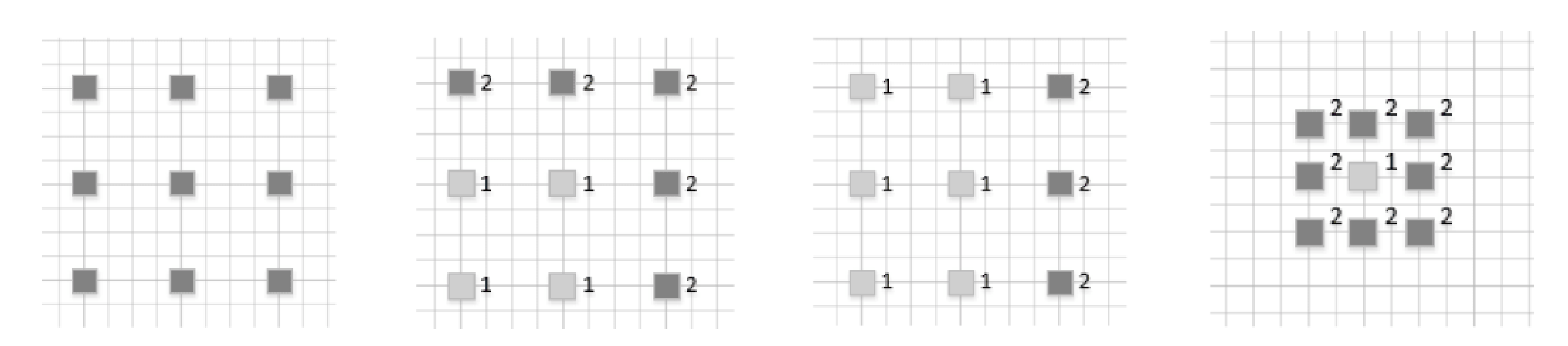


图 8-8　四步搜索法可能的搜索位置

8.3.5　基于块的梯度下降搜索法

基于块的梯度下降搜索法(Block-Based Gradient Descent Search，BBGDS)利用运动矢量中心分布特性，在搜索过程中使用 3×3 搜索窗口。视频帧内相邻像素间具有渐变性，每一步的最小块失真点分布具有一定的方向性，即梯度下降方向。基于块的梯度下降搜索法使用梯度下降方向决定下一步的搜索方向，如图 8-9 所示。

图 8-9 表示了基于块的梯度下降搜索法的搜索过程。在每一步搜索过程中，基于块的梯度下降搜索法引入梯度下降的概念，用梯度下降的方向指导搜索方向，对该方向进行重点搜索，从而减少和避免了不必要的搜索，大大降低了算法的复杂度。

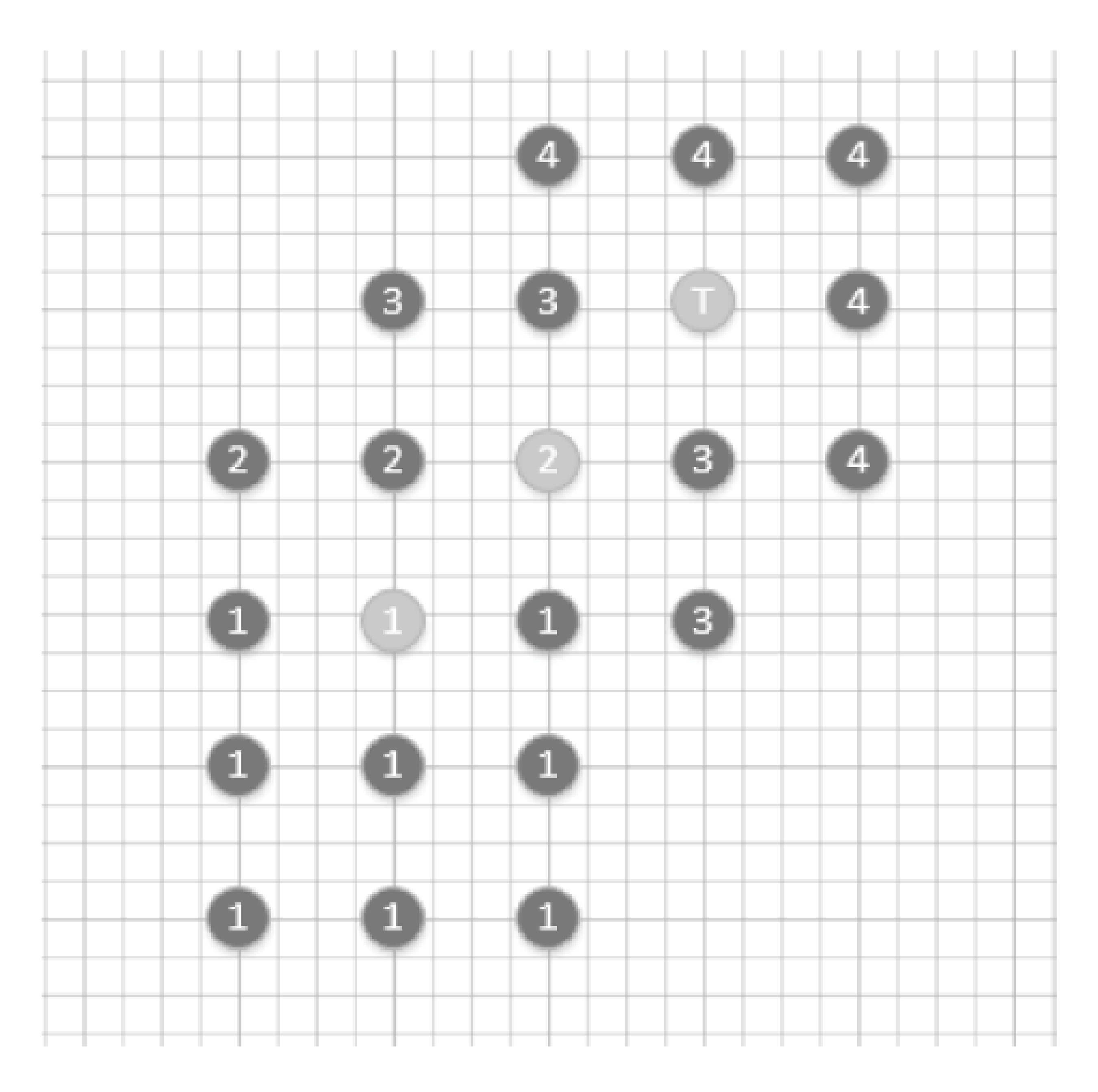


图 8-9　基于块的梯度下降搜索法

8.3.6　菱形搜索法

菱形搜索(Diamond Search,DS)法最早由 Shan Zhu 和 Kai-Kuang Ma 两人提出,后经过多次改进,已成为目前快速匹配算法中性能最优异的算法之一,现在已被 MPEG-4 国际标准采纳并收入验证模型。

基于这两点事实,菱形搜索法采用了两种搜索模板,分别是有 9 个检测点的大菱形搜索模板(Large Diamond Search Pattern,LDSP)和有 5 个检测点的小菱形搜索模板(Small Diamond Search Pattern,SDSP),如图 8-10 所示。

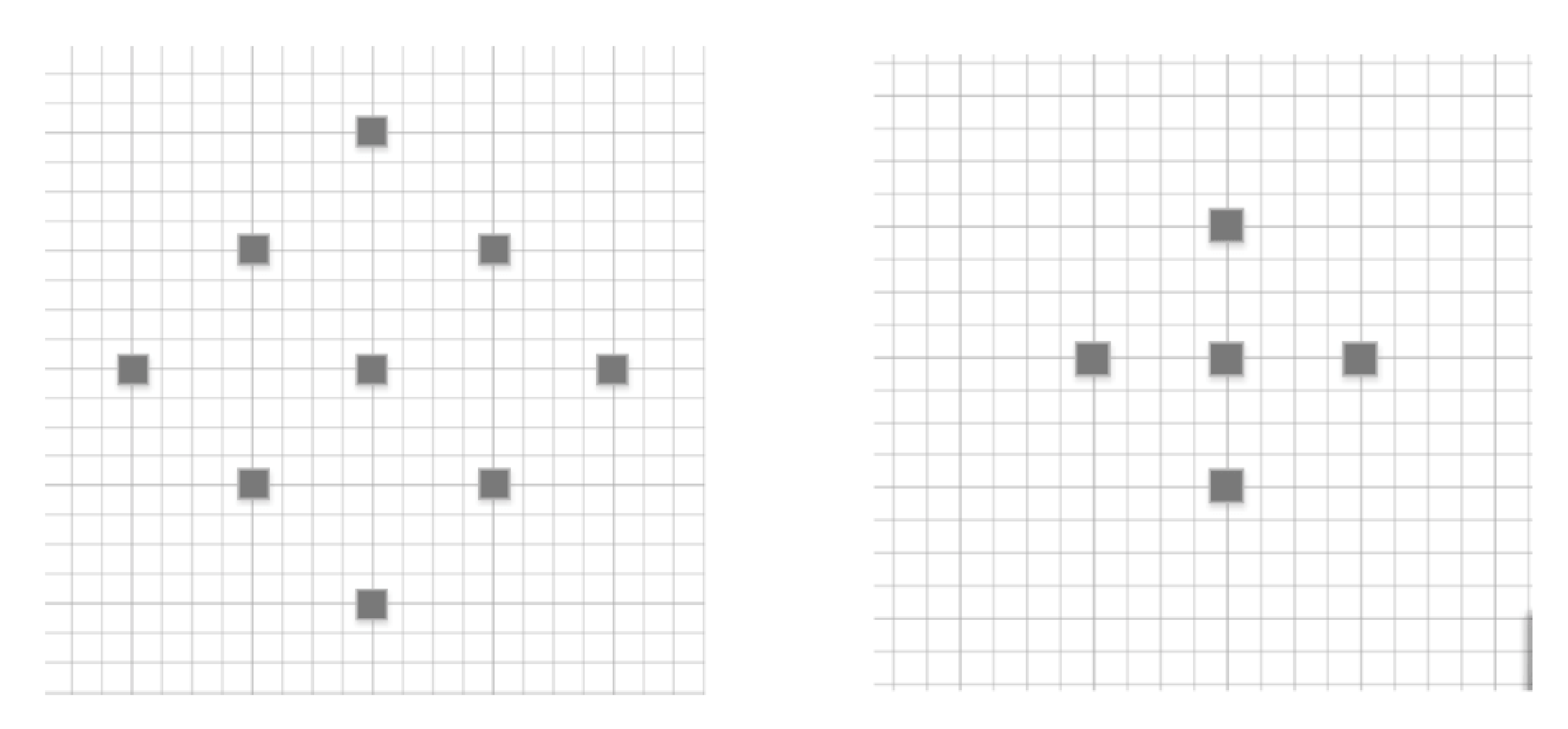


图 8-10　搜索法的两种搜索模板

在菱形搜索法过程中,大菱形模板被重复使用,直到最小块失真点出现在中心点。然后搜索模式由大菱形模板转换为小菱形模板,进入最后的搜索阶段。在小菱形模板的 5 个检测点中,出现最小块失真点的位置就确定了运动矢量,如图 8-11 所示。

菱形搜索法的特点在于它分析了视频图像中运动矢量的基本规律,选用了大小两种形状的搜索模板:大菱形搜索模板和小菱形搜索模板。先用大菱形搜索模板进行搜索,

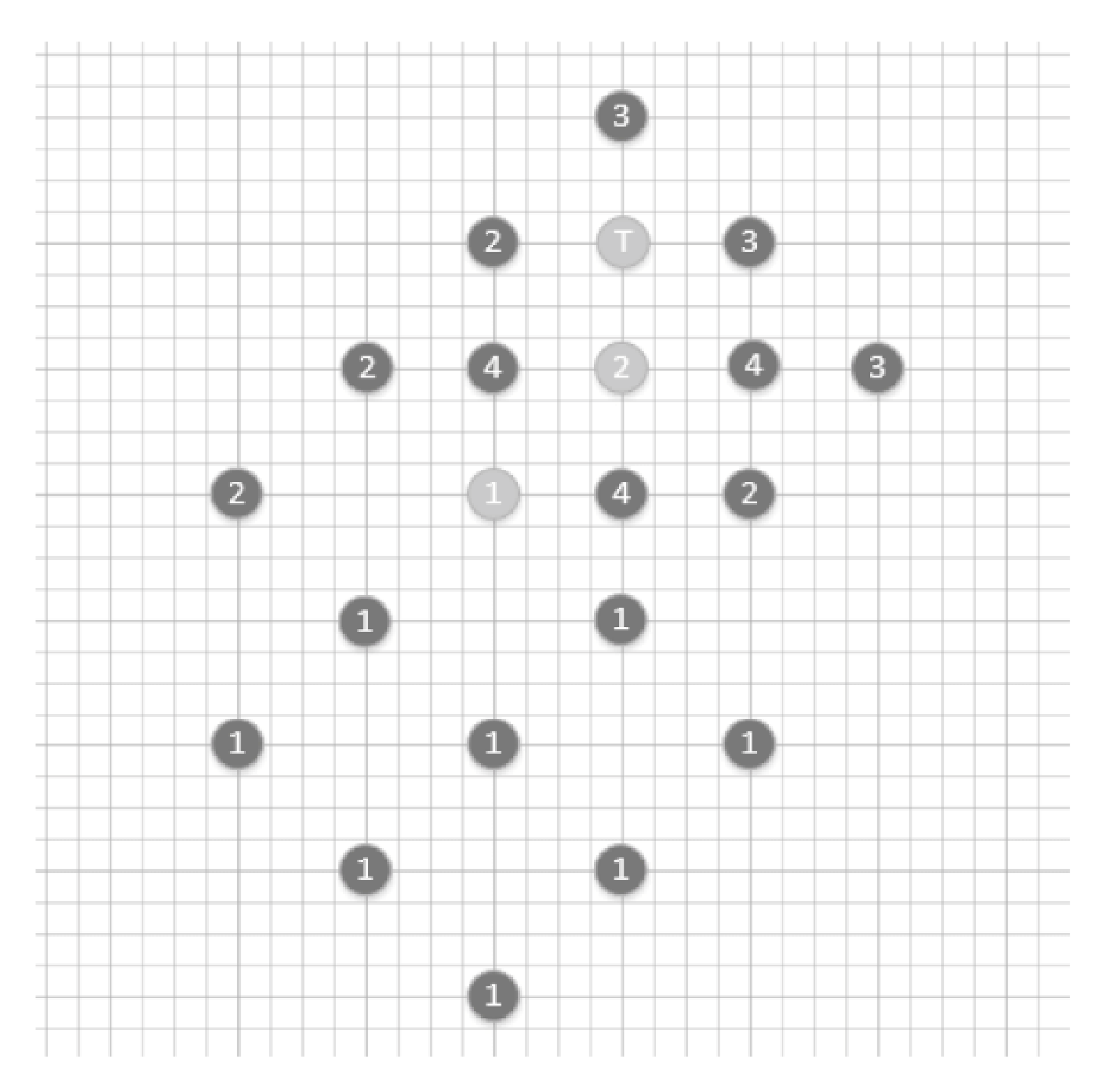


图 8-11　菱形搜索法搜索过程示意图

由于步长大，搜索范围广，因此可进行粗定位，使搜索过程不会陷入局部最小；当粗定位结束后，可以认为最优点就在大菱形搜索模板周围 8 个点所围的菱形区域内，这时再用小菱形模板准确定位，使搜索不至于有大的起伏，所以它的性能优于其他算法。另外，菱形搜索法搜索时各步骤之间有很强的相关性，模板移动时只需在几个新的检测点处进行匹配计算，所以也提高了搜索速度。

8.4　基于 MPEG-2/4 视频流的水印方案

通过分析现有的数字视频系统，按照水印在视频码流处理中嵌入的位置，可以将目前的视频水印大体上分为以下 5 种方案，如图 8-12 示。

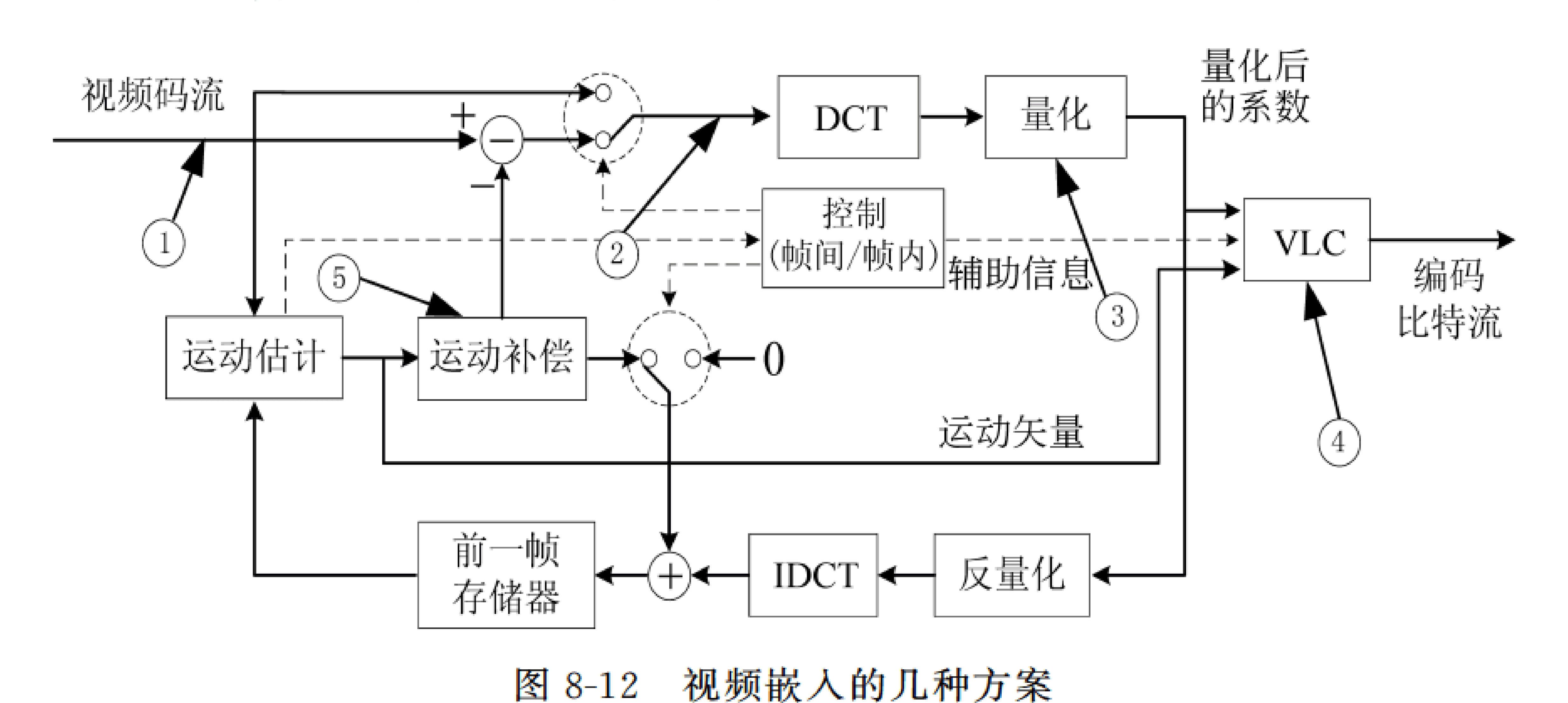


图 8-12　视频嵌入的几种方案

（1）水印直接嵌入在原始视频码流中。此类方案的优点是：水印嵌入的方法比较

多,很多数字图像水印方案都可以应用于此。缺点是:会增加视频码流的数据比特率;经过 MPEG-2 压缩后会造成水印信息的丢失;高的视频压缩率会降低图像的质量。

(2) 水印嵌入在编码阶段(DCT、DFT、DWT)的等变换域的系数中。此类方案的优点是:水印仅嵌入在系数的量化中,不会增加视频流的数据比特率;易设计出抗多种攻击的水印。缺点是:会降低视频的质量,因为一般它也有一个解码、嵌入、再编码的过程。

(3) 水印的嵌入和 DCT 量化编码相结合。这种方案一般多是构造脆弱性的方案。其优点是:容易和编/纠错码相结合。缺点是:鲁棒性差。

(4) 水印直接嵌入在 MPEG-2 压缩比特流中。此类方案的优点是:没有解码和再编码的过程,因而不会造成视频质量的下降,同时计算复杂度低。缺点是:由于压缩比特率的限制而限定了嵌入水印的数据量的大小。

(5) 被加的水印信号大小依赖于对未水印化和水印化序列的运动补偿的差分估计。尽管视频的比特流因加水印必须被分解而且水印必须进行 DCT,但是该方法不要求完全的解压缩和再压缩。该方案的鲁棒性尚待证明。

8.5 数字视频水印应具有的特征

由于 Video 具有的数据量大,在具体的应用中往往将图像序列以压缩编码的方式进行存储和传输,因此,相关的视频水印必须针对具体的压缩标准进行算法设计,同时还期望具备以下许多不同的特征[169,170]。

- 不可视性:嵌入在 Video 中的水印必须是感官察觉不到的。
- 安全性:算法公开,在正确的参数未知的情况下,对水印的删除是不可能的。
- 鲁棒性:在压缩的和未压缩的 Video 流上通过有意或无意对水印的处理是不可能的。与此同时,显著降低视觉质量将影响其商业价值,这些操作包括加入信号、滤波、剪裁、编码或者模拟记录以及回放。
- 复杂性:水印及水印恢复理论上要具有低的复杂性。如果水印用于跟踪,每一接收者对于水印的提取必须简单,如果水印是用在 Video 中嵌入用户的个人身份商标,那么商标需要嵌入在大量分发的 Video 序列中。为了解决对水印的各种可能的攻击,算法的复杂度要低。
- 抗压缩处理:数字 Video 通常会以压缩的形式发送或转存(例如在请求服务器上,或者在万维网服务器上),这样对嵌入在压缩的 Video 流中的水印信息将是一个严峻的考验。
- 恒定的比特率:在比特流中加入水印不能增加整个视频传输的比特率,至少应符合通信传输带宽的要求。

由于具体的应用目的及环境的不同,以上对视频水印的不同要求在具体的水印方案中有可能不需要同时满足,这几种要求在某些情况下存在着折中。

8.6 视频水印嵌入方案

我们仅在 I 帧中加入水印，是由于 I 帧是 Video 流中最显著，也是最重要的帧。因为 I、B、P 之间的关系，I 帧的水印将扩散到 B 和 P 帧中。攻击者如果将所有 Video 流中的 I 帧变弱，的确可以将水印信号从 Video 中删除。但如果 I 帧的信号变弱，B 或者 P 帧的质量将严重下降。而在 I 帧中，仅在亮度的 8×8 块中加入水印，因为亮度信号比其他两个色度信号强得多。其次，加水印开始于原始的数据流中，可以预设一种 MPEG 的编码码流格式，将水印嵌入在所选定帧中的 DCT 块的中频 AC 系数中。

在本书的方案中，首先对原始 Video 序列的内容进行分析，在基于 MPEG 编码格式的图像流中，对所有 I 帧图像的动态进行检测，选择变化大的序列帧图像嵌入水印；利用混沌映射将水印商标在空间域上进行置乱，然后将置乱的水印商标分块嵌入在选择的相应图像的 DCT 分块系数中，这样，攻击者对水印信息的预测是困难的；通过提取图像的模糊熵测度准确描述 Video 图像中适合信息隐藏的显著特征，利用图像模糊熵和帧图像的局部变化确定水印的嵌入权值。对水印商标的检测，不需要原始的序列数据，利用 Kalman 滤波预测嵌入的信息，从而使商标得到很好的恢复，以表明产品的版权。该方案基于 MPEG-2 压缩标准，但是也可应用于其他的混合编码方式中。

8.6.1 水印商标的产生及嵌入

在文献[171]中，作者提出用不相关的伪随机噪声(PN)矩阵和参考的水印图案相乘，不管是 PN 矩阵，或者是嵌入的水印，在接收端是知道的。值得注意的是，对于 Video 序列的每一帧水印都是相同的，而 PN 矩阵是不同的，这保证商标的空间位置在不同的帧不同，从而保证水印的安全性。另一种常用的方法是将用户 ID 或者商标在空间域上转换成扩频信号，然后再嵌入 Video 中，这种方案在原理上和文献[169]中的方法基本相同。在本方案中，水印商标是通过第 3 章介绍的空间域的混沌映射的方法产生的，混沌映射的参数 k 可以被看作用户的私钥。经过迭代置乱后的商标在空间域上要比原始商标大得多，但基本的像素数一样。因此，商标的置乱映射可以被看作空间域上的一个“疏”映射，由于 Video 可供嵌入的像素很多，考虑将置乱后的商标从空间域上可以分成若干小的子块，这些子块的数量可根据要嵌入的视频序列的具体特点，单帧图像能够携带的信息量以及压缩率等因素确定。水印商标的产生及嵌入如图 8-13 所示。

8.6.2 序列帧图像的动态特征检测

一帧图像中运动的分布情况：运动程度在视频质量评价过程中起着重要的作用。运动矢量描述了当前帧宏块与上一帧最相似图像块之间的偏移[171]。可以利用各宏块运动矢量的长度定义一帧图像中运动的分布情况。

令$[\Delta x_k(i,j), \Delta y_k(i,j)]$表示第 k 帧中宏块(i,j)的运动矢量。那么，该宏块的运动程度用式(8-6)定义。

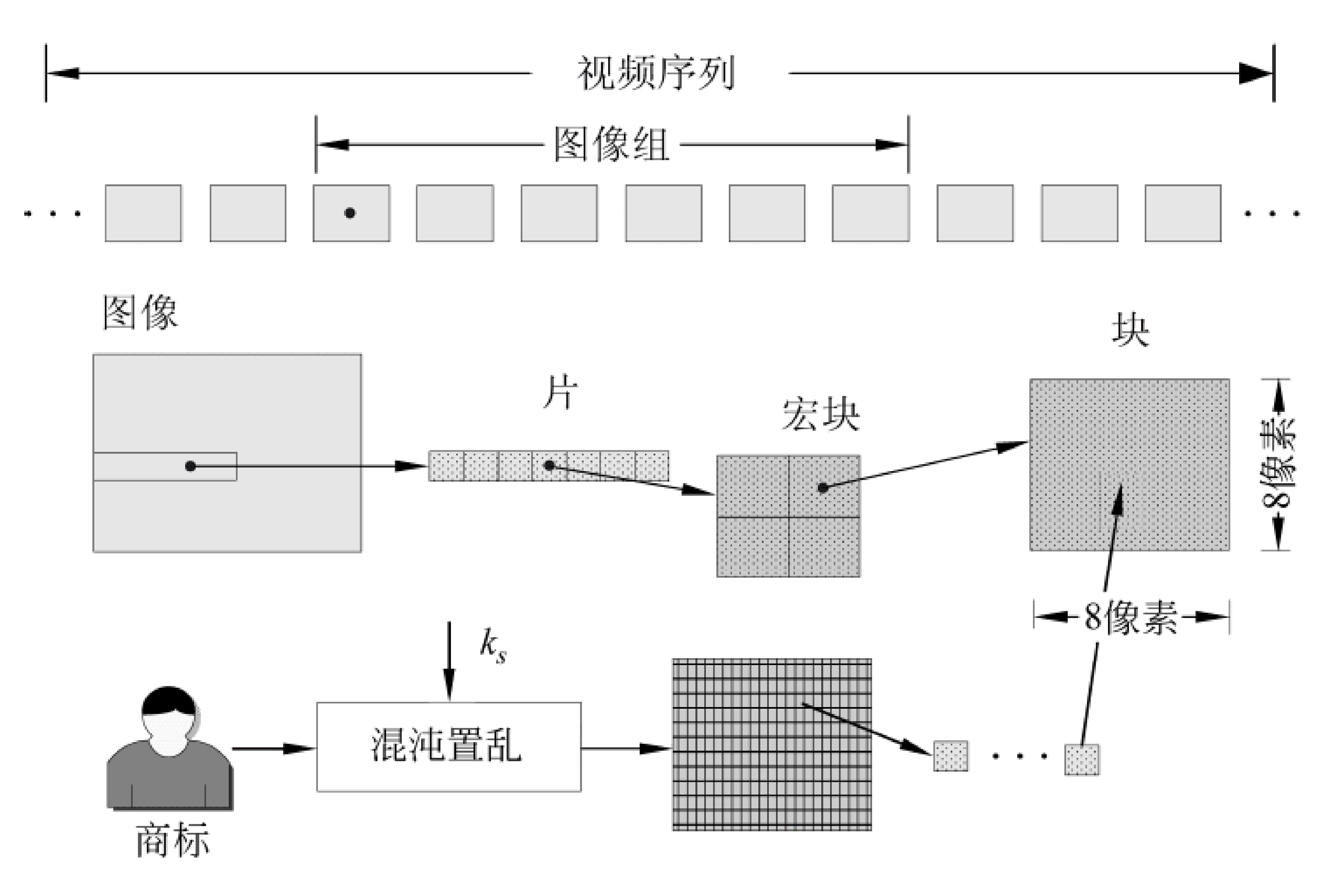


图 8-13　水印商标的产生及嵌入

$$A_{M,k}(i,j) = 1 + \frac{1}{A_{M,\max}}\sqrt{\Delta x_k^2(i,j) + \Delta y_k^2(i,j)} \tag{8-6}$$

其中，$A_{M,\max}$表示运动矢量的最大可能长度值。相应的该帧图像的整体运动剧烈程度$A_{M,k}$由式(8-7)定义。

$$A_{M,k} = \frac{1}{N_{M,B}}\sum_i\sum_j A_{M,k}(i,j) \tag{8-7}$$

其中，$N_{M,B}$表示一帧图像中的宏块个数。

各帧的运动分布：基于两帧误差，就是利用两帧之间的绝对误差帧描述一帧图像的运动程度。

令 $L_k(m,n)$表示第 k 帧中像素(m,n)的亮度值。第 k 帧中宏块(i,j)的运动程度可用式(8-8)定义。

$$A_{M,k}(i,j) = 1 + \frac{1}{N_p}\sum_{(m,n)\in \mathrm{block}(i,j)} \left| L_k(m,n) - L_{k-1}(m,n) \right| \tag{8-8}$$

运动较剧烈的清晰度对整段视频清晰度的贡献较弱。因为运动剧烈，所以人眼可能分辨不出该帧中太多的细节。因此，在帧图像序列中嵌入水印，需要对帧序列的每一帧图像中以及帧图像中之间的运动进行检测，从人眼的视觉特征讲，在这些运动较为剧烈的部分帧中应该嵌入相对比较多的水印信息，水印的强度相对更大。而对具体的一帧图像，其特征的检测可参考第 3 章对图像特征的检测。实际上，模糊熵反映了图像像素之间的变化程度。也可以说，图像的一些特征分布明显的区域，诸如纹理、边缘区域或者活动性强的区域的模糊熵值较大，将水印信息嵌入在这些区域有利于提高水印的鲁棒性。

8.6.3　水印的嵌入步骤

(1) 对原始的序列进行动态特征分析，利用 8.6.2 节的式(8-6)和式(8-7)，对所有编码结构中的 I 帧的运动特性进行排序，找出动态变化大的图像作为水印化的帧。每一帧中图像的变化程度可参考式(8-8)。

(2) 考虑一幅 I 帧的亮度信号 $\{f_i[n_1, n_2], i=1,2,\cdots,M\}$，由 M 个大小为 $N_1\times N_2$ 的单帧图像 $f_i[n_1, n_2]$ 组成，用 $w_i^{(s)}[k_1, k_2]$ 表示第 k 帧中所要嵌入的水印信息。

(3) 将 $f_i[n_1, n_2]$ 分解成互不重叠的 8×8 的图像块 $B_i^{(k)}(u, v)$，$u, v=1,2,\cdots,8$；$k=1,2,\cdots, N$。N 是能分成块的个数，用模糊熵测度的算法对整个图像上分块的模糊熵进行统计检测，水印只嵌入在模糊熵大的块中。设置门限 τ 及水印标志位 $b_i^{(k)}$，检测 R_{B_k}，若 $R_{B_k}>\tau$，则 $b_i^{(k)}=1$，否则 $b_i^{(k)}=0$ 。τ 的值可以根据嵌入的信息量自适应地调整。

(4) 用 $C^{(k)}(u_1, v_1)=\mathrm{DCT}[B_i^{(k)}(u, v)]$ 表示第 i 帧图像中 $B_i^{(k)}(u, v)$ 块的 DCT 系数。$u_1, v_1=1,2,\cdots,8$；$u, v=1,2,\cdots,8$；$k=1,2,\cdots, N$。将置乱的水印商标 W 分成许多 4×4 大小的子块，各个子块按顺序分别嵌入在不同帧中的 $b_i^{(k)}=1$ 的 DCT 系数块中，水印权值的确定可参考 4.2.5 节，得到的权值乘以模糊熵的值，再经过全局因子调整加权相应的水印信息，形成水印化的系数 $C_w^{(k)}(u_1, v_1)$。

(5) 用 $C_w^{(k)}(u_1,v_1)$ 代替 $B_i^{(k)}(u,v)$，然后进行 DCT 的逆变换，将逆变换的块进行重新排列形成水印化的图像块 $f_i^w[n_1,n_2]$，而所有水印化的帧以及没有水印化的帧形成了加水印的 Video 序列。

8.6.4 水印的检测与提取

水印的检测与序列的重新解码和重构相结合，如图 8-14 编码的比特流经 VLC 解码后，将嵌入的水印的那些特征系数输入到 Kalman 滤波器中，滤波器的另一端是由用户提供的参考序列，经过预测滤波恢复出每一帧中的水印，这些水印块可形成重构的商标。在没有原始数据的情况下，对于 Video 水印的检测，利用 Kalman 预测对嵌入的水印信号进行滤波。

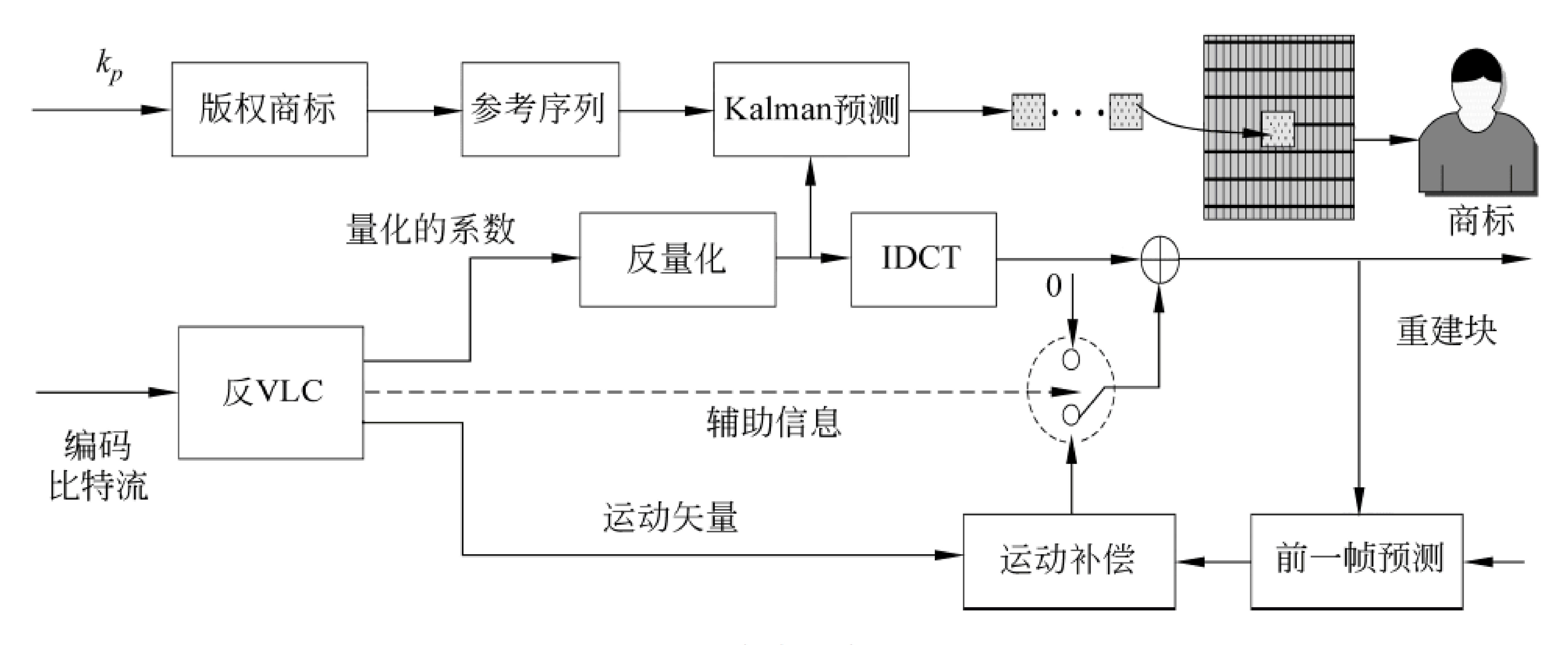


图 8-14　水印的提取流程

商标的重构基于滤波器从水印化的序列中对嵌入的置乱信息的检测估计，从每一水印化的帧中检测出嵌入的部分商标的信息，按顺序将各个帧中的信息重新排列，形成混乱的商标图像 w'，利用映射 $A_N^{-1}(k)$ 对 w' 中的空间坐标进行迭代逆映射回原始位置，相应位置的像素值进行交换。

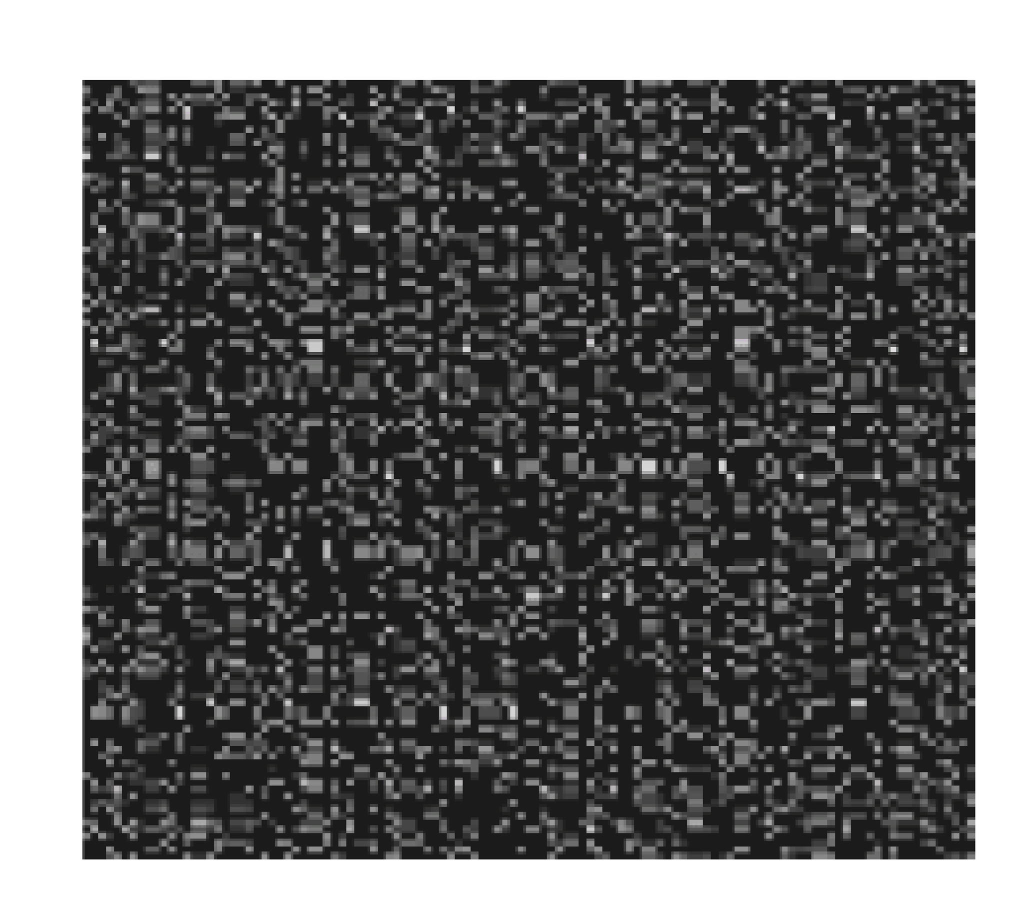
8.7　模拟试验结果

用两个 QCIF 格式的 Susie 和 Claire Video 序列进行实验，图像的大小为 144×176 像素，整个水印的嵌入及检测算法基于图像的 8×8 像素分块，选择 YAHOO 作为二进制的水印商标，其大小为 40×140 像素。嵌入之前，先使用商标混沌映射将其在空间域中置乱，映射参数取 $k=11$，$N=240$，$n=87$，获得置乱的商标的大小为 240×240 像素，这里将 240×240 像素的商标分成 60×60 像素大小的子商标，这样总共可分成 16 个子商标，将这 16 个子商标分别嵌入在 Video 序列的 16 个 I 帧图像中。而在每一帧图像的 8×8 像素的分块中，只改变其中的 16 个中频 AC 系数的值，这 16 个像素对应的坐标为(3～6，3～6)，在一帧图形中需要 225 个 8×8 像素的分块，而一帧图像最多可能的分块为 176×144/(8×8)=352，在 352 块中选择 225 块嵌入水印。为了构造鲁棒性的水印，只选择模糊熵测度大的图像块嵌入水印，算法中的门限值可根据嵌入水印的比特数自适应调节。

图 8-15 为原始的水印商标及置乱后的水印商标。在没有原始映射参数的情况下，想从图 8-15(b)逆映射回图 8-15(a)是困难的，而且知道图 8-15(b)并不能分辨出图 8-15(a)。



(a) 原始的水印商标



(b) 置乱后的水印商标

图 8-15　原始的水印商标及置乱后的水印商标

图 8-16 为帧图像的模糊熵及水印的分布效果。图 8-16(a)为 Susie 序列中水印化的一帧图像的模糊熵的分布。图 8-16(b)为在单帧图像的水印的分布。为了显示水印分布的区域，在实验中，我们有意放大了水印的嵌入权值，选 $\lambda=3$，从实验结果看，水印明显嵌入在图像的边沿及纹理变化强烈的地方。

图 8-17 为水印 PSNR 及相关检测结果。图 8-17(a)是两个序列中水印化各 I 帧的 PSNR(dB)的值($\lambda=0.3$)。图 8-17(b)为两个序列水印化帧的相关系数的检测结果。如果提供的水印和图像中的水印不相关，则系数范围 0～0.2 随机分布，而在相关情况下，则如图 8-17(b)中的测试结果。

图 8-18 是在 Susie 序列中对水印的相关峰值的检测结果，检测只提供原始水印信息

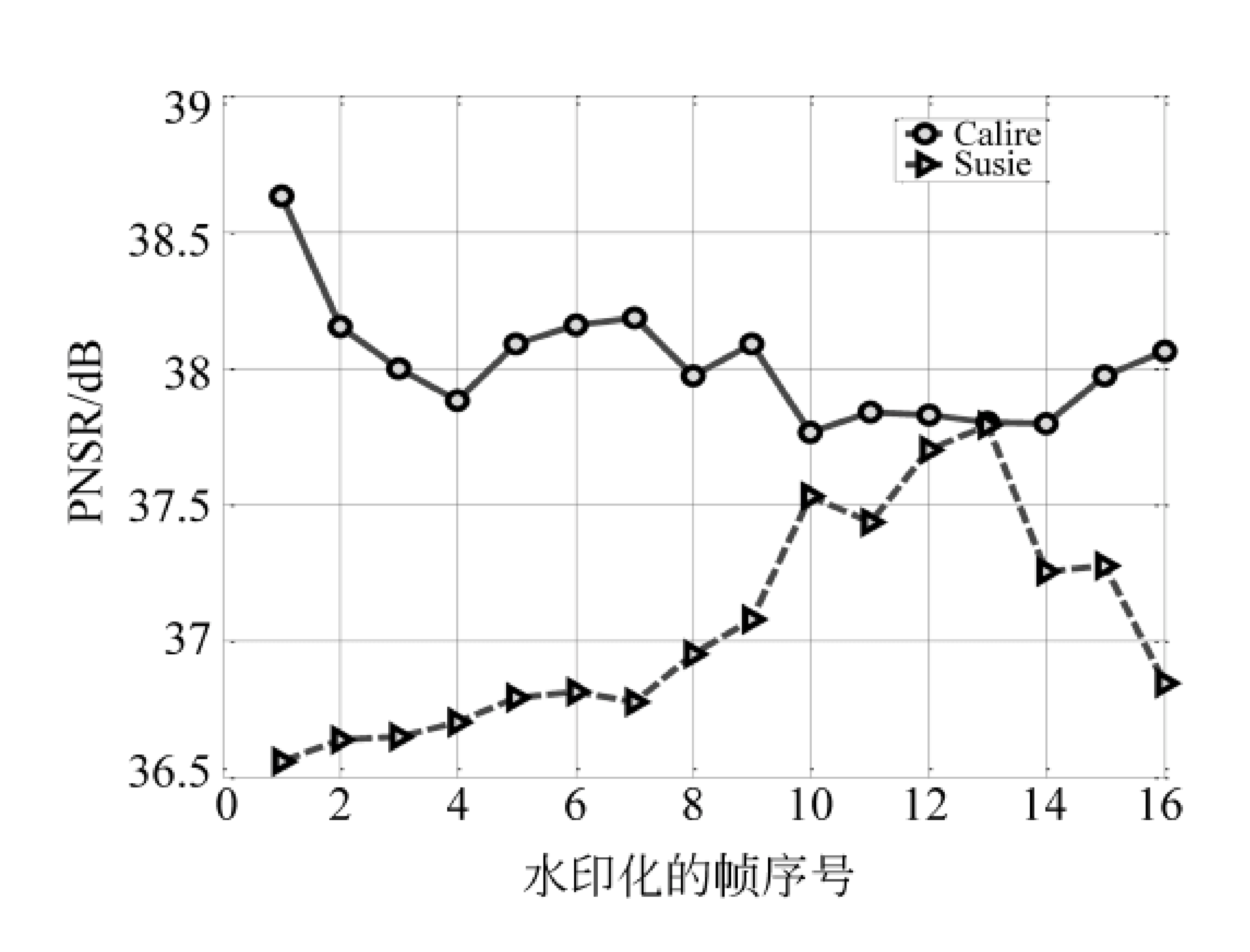


(a) 其中 I 帧的模糊分布



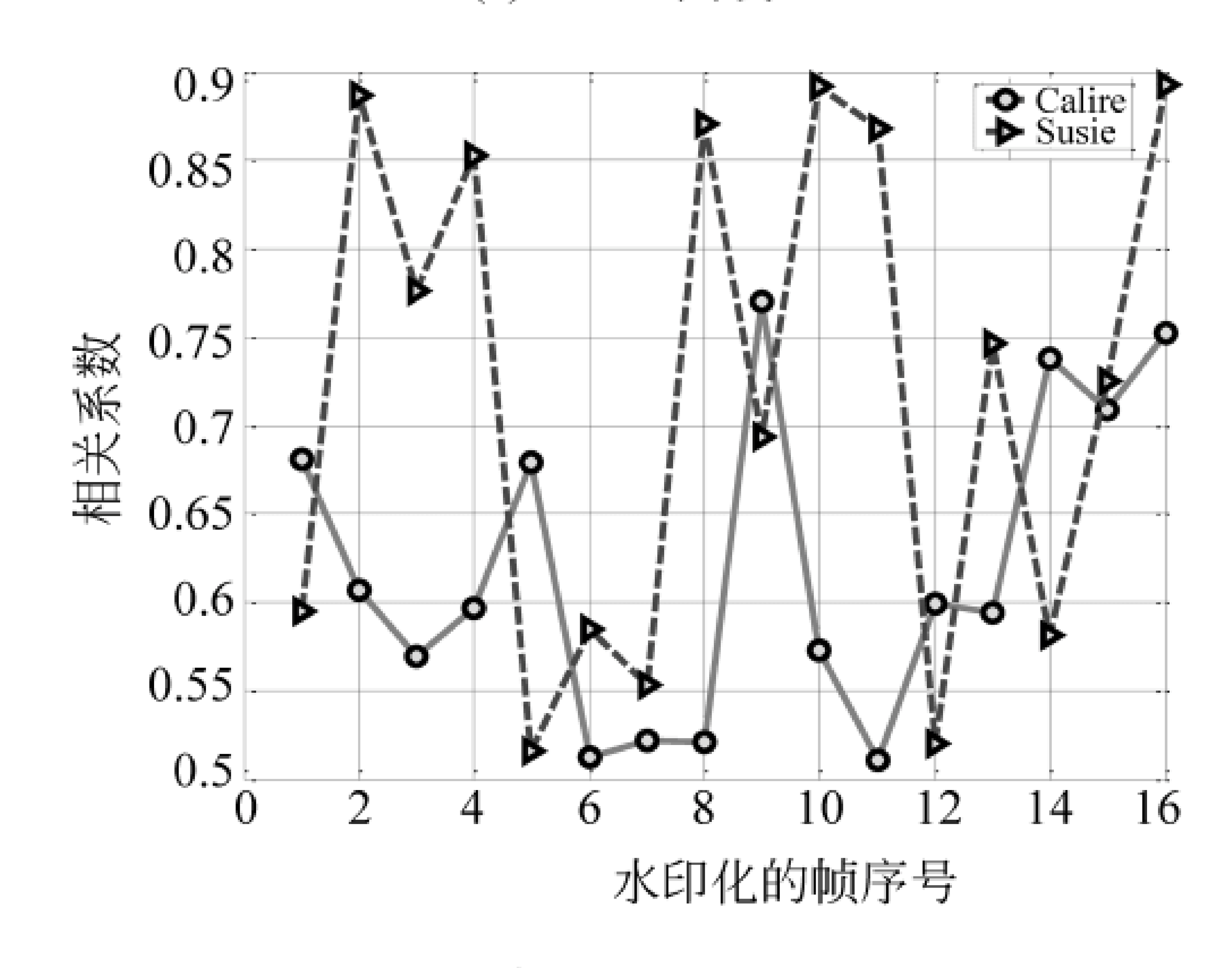
(b) 水印的分布

图 8-16　帧图像的模糊熵及水印的分布效果





(a) PSNR 曲线



(b) 相关系数曲线

图 8-17　水印 PSNR 及相关检测结果

(这里可以是置乱的商标)。

图 8-19 显示了水印化对各种帧图像带来的影响。在 MPEG-2 的 Video 通用压缩编码格式下,因为 P 帧和 B 帧都是从 I 帧中预测而来,在 I 帧加入水印引起的图像的失真肯定会引起相关帧图像的失真。由图 8-19 可看出,预测的关系对各帧带来的误差不完全相同,而且相关图像的失真是累积的。

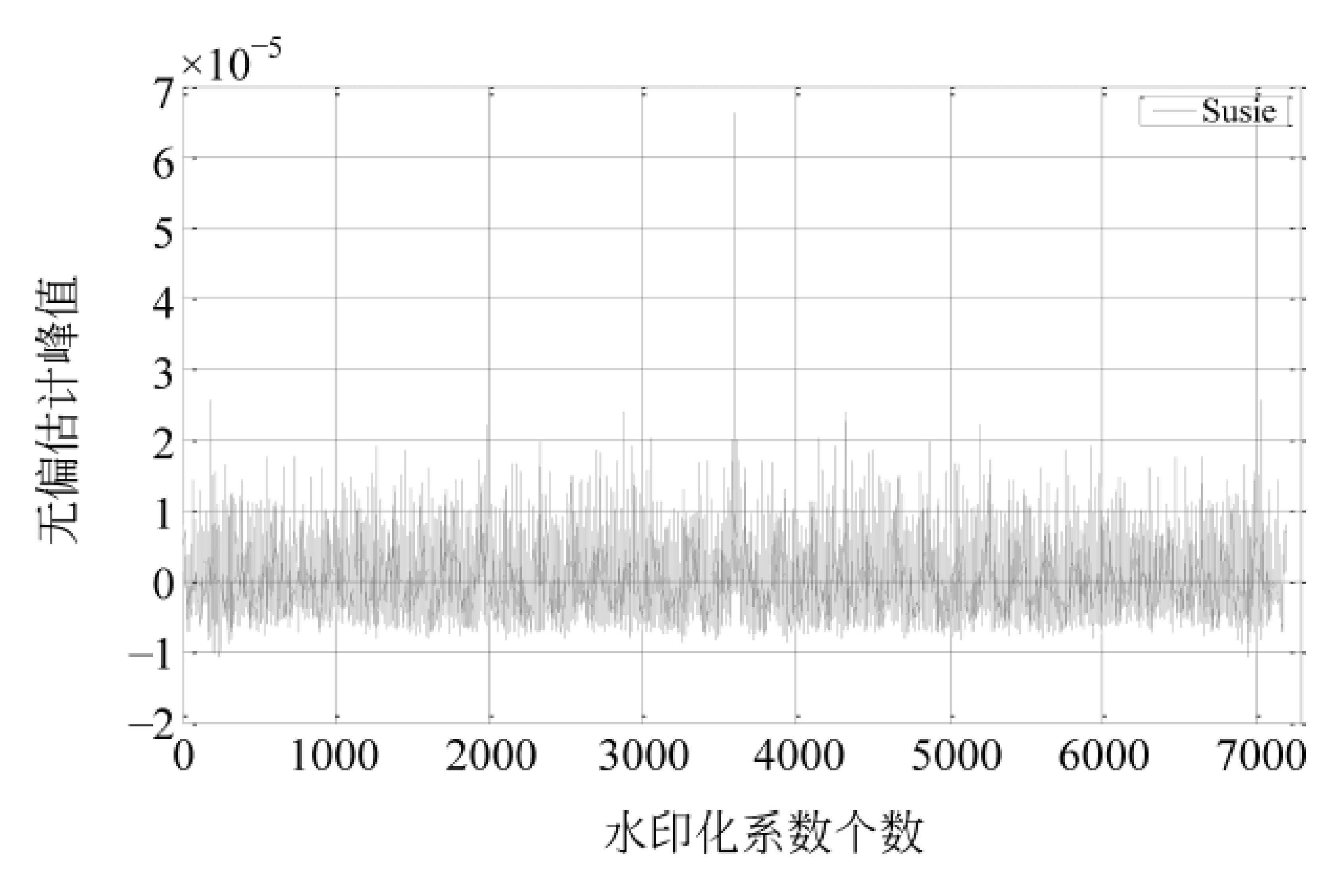


图 8-18　相关峰值的估计

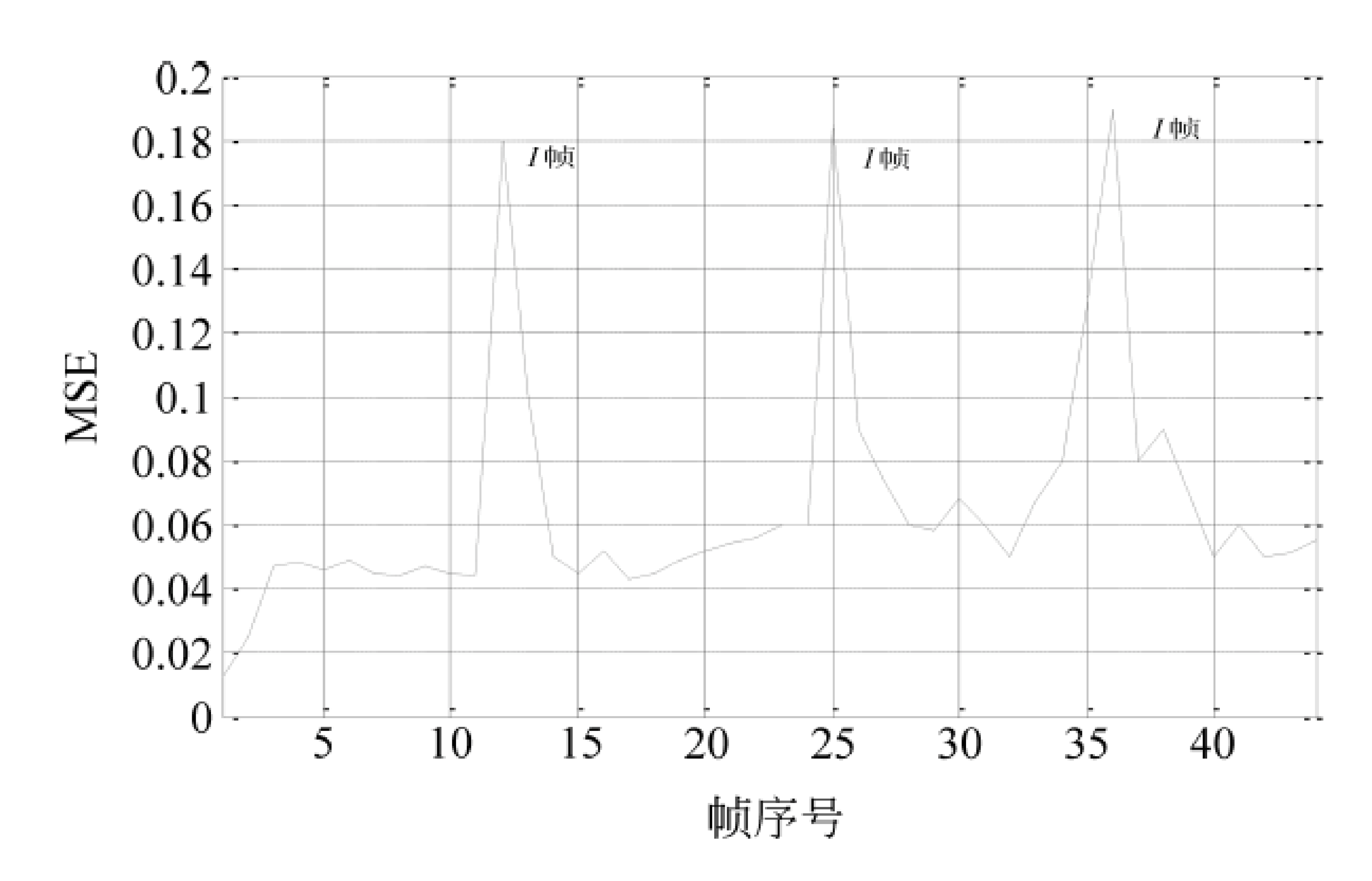
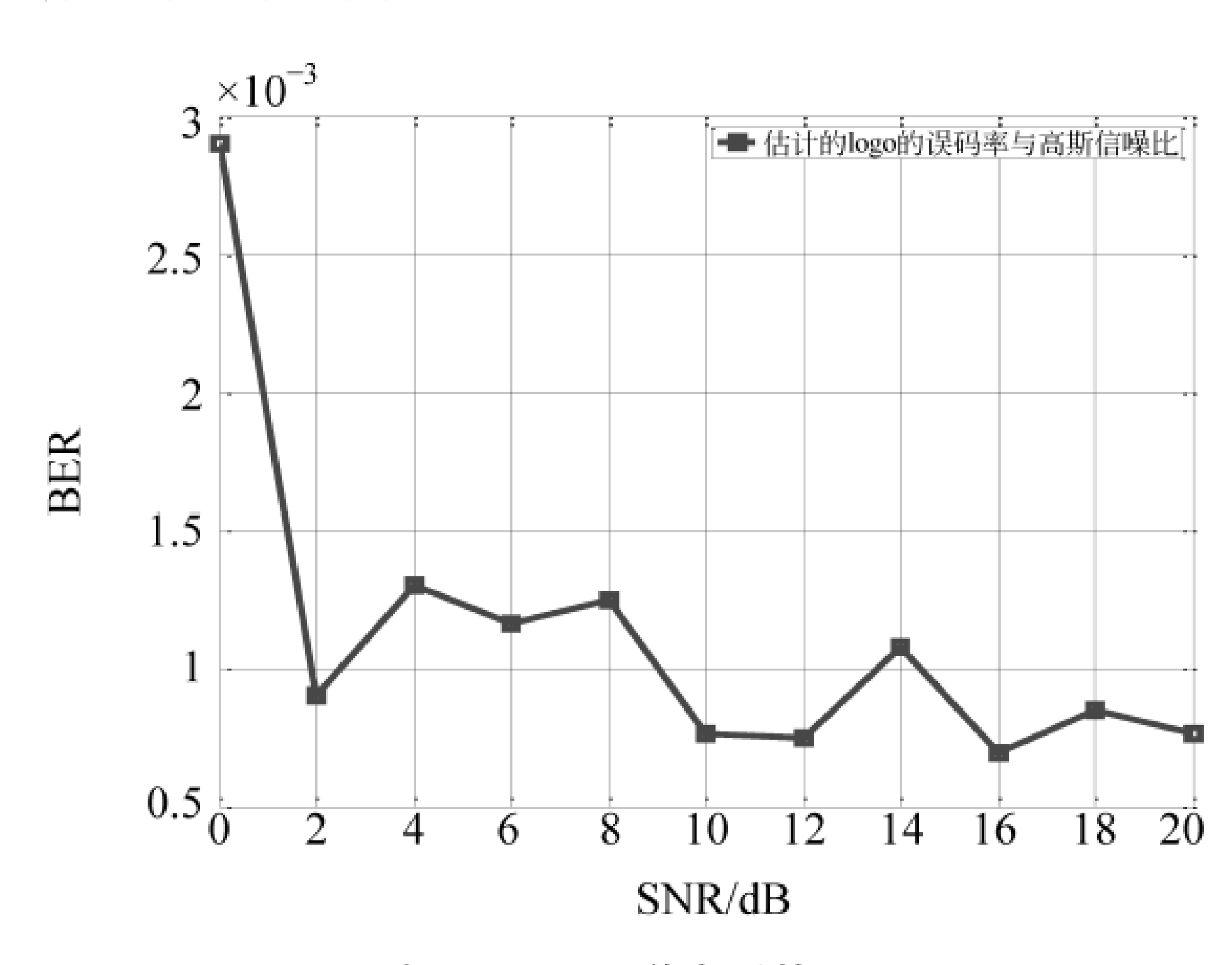


图 8-19　水印化序列帧的平均误差

图 8-20 是采用 Kalman 滤波器对嵌入的水印信息的检测，商标的恢复和重构基于滤波器的输出结果。实验中，我们在水印化的序列中加入了 30dB 噪声，检测重构的水印商标如图 8-20(a)所示。为了检验在加噪情况下水印商标的检测效果，我们在水印化的序列中加入了一定的高斯噪声，信噪比和检测错误率的关系如图 8-20(b)所示。



(a) Kalman 检测结果(SNR=30dB)



(b) 加 Gaussian 噪声后的BER

图 8-20　Kalman 滤波结果

图 8-21 为剪裁及压缩后的结果。对于帧剪裁和丢失的情况，我们从水印化的帧中删除 3 帧，而用随机数代替，其水印恢复的结果如图 8-21(a)所示。商标的恢复依然可见，其原因是，在我们的方案中，原始商标映射后分块分别嵌入在 Video 序列中，对单帧的删除，只能部分删除商标信息，因此本方案是抗帧剪裁和丢失的。

在大多数应用场合，数字 Video 涉及存储及传输，因此常常将 Video 序列进行有损压缩和编码。为了检验 MPEG 压缩编码对水印的影响，我们采用 MPEG-2 默认的基于 HVS 的量化门限乘以 3/4 因子对水印化的 Video 序列进行量化和 Huffman 编码，相应的压缩比率(CR)为 5.6∶1，然后另存、解压缩。图 8-21(b)为压缩后的水印化 Video 序列中的一帧图像，此时图像中水印是无感觉的，水印商标依然可检测。将恢复的水印序列在专用的播放器中播放，其效果和原始的序列相比，图像质量没有明显差别。



(a) 帧剪裁后商标的恢复



(b) 压缩后的 I 帧图像

图 8-21　剪裁及压缩后的结果

第 9 章 自然语言文本隐藏

摘要：本章给出了一种基于中文同义词替换的隐藏算法，详细介绍了分词系统、同义词词库的构建以及同义词词组的编码算法，给出了基于中文同义词替换的编码隐藏系统。

9.1 二次剩余理论

在基于同义词替换的隐藏算法中，利用二次剩余随机选择将被隐藏的同义词，这样可以增强该算法的抗攻击能力。在此首先介绍二次剩余的定义。

定义 9.1 设 m 是大于 1 的正整数，若同余式

$$x^2 \equiv a(\text{mod } m) \quad (a,m)=1 \tag{9-1}$$

有解，则称 a 为模 m 的平方剩余(或二次剩余)；否则称 a 为模 m 的平方非剩余(或二次非剩余)。

例如：$m=11$，求出模 m 的二次剩余和二次非剩余，见表 9-1。

表 9-1 二次剩余(mod 11)

j	±1	±2	±3	±4	±5
$a=j^2$ mod 11	1	4	9	5	3

由表 9-1 可以看出，模 11 的二次剩余为 1,3,4,5,9；二次非剩余为 2,6,7,8,10。

二次剩余理论中有一个重要的结论：在模 m 的一个既约剩余系中，恰有 $(m-1)/2$ 个模 m 的二次剩余，$(m-1)/2$ 个模 m 的二次非剩余。也就是说，模 m 的二次剩余和二次非剩余的个数是相等的，因此可以采用二次剩余理论选取所有待隐藏的一个子集，将所有结点编码为 0 或 1，0 代表该结点标记的是模密钥的二次剩余，1 代表该结点标记的是模密钥的非二次剩余，然后根据待隐藏位出现的位置上的编码是 0，还是 1 选择该位置上的结点是否作为隐藏位。

9.2 分词系统及同义词词库

9.2.1 分词系统

在汉语的书面表达中，单字是最小的单位，词与词之间并没有明显的界限标志。因此，

在汉语文本分析处理中，分词是首先要解决的问题。中文分词(Chinese Word Segmentation)是指将一个汉字序列切分成一个个单独的词，词的字数最小为1，此时为单字。

在汉语中，字、句和段落可以通过明显的分界符(如标点、回车等)划分，但是词却没有一个形式上的分界符。因此，在以词为单位的文本处理就显得更复杂，一个好的分词系统对于文本处理就显得尤为重要。目前，分词的算法主要有基于字符串匹配、基于理解和基于统计的分词3种方法。

哈尔滨工业大学信息检索研究中心(HIT-CIR)语言技术平台[172]是哈尔滨工业大学信息检索实验室开发的一套中文语言处理平台，免费提供给高校和科研院所用于科学研究。它的语料资源主要来自哈尔滨工业大学信息检索研究中心汉语依存树库(HIT-CIR Chinese Dependency Treebank)和哈尔滨工业大学信息检索研究中心同义词词林扩展版(HIT-CIR Tongyici Cilin(Extended))；其中的语言处理模块包括断句(Sectence Splitting，SplitSectence)、语法分析(Lexical Analysis System，IRLAS)、基于SVMTool的词性标注(Part-of-Speech Tagging，PosTag)、命名实体识别(Named Entity Recognition，NER)、基于动态局部优化的依存句法分析(Dependency Parsing，Parser)、全文词义消歧(Word Sense Disambiguation，WSD)等，涉及中文处理的各个领域，可以达到很好的分词效果和较高的效率。本实验借助这个语言技术平台以句子为单位的处理模块进行分词，借助count模块依次处理每个分词并进行统计与编码。系统调用的接口主要如下。

```
//从句子创建 DOM
CreateDOMFromString(const char * );
//调用以句子为单位的处理模块
int SplitSentence();
//分词
int SegmentWord();
//查看某一个段落的句子数，paragraphIdx 为段落号，从 0 开始编号
int CountSentenceInParagraph(int paragraphIdx);
//查看第 paragraphIdx 个段落中的第 sentenceIdx 个句子的词语数，sentenceIdx 为句子
//在段落中的编号，从 0 开始编号
int CountWordInSentence(int paragraphIdx, int sentenceIdx);
```

9.2.2 同义词词库的构建与编码

1. 同义词词库的构建

以《同义词词林》为基础构建中文同义词库。最原始的《同义词词林》是由梅家驹等人[173]于1983年编撰而成的，初衷是对创作和翻译等工作提供同义词组，后来被用于信息处理中，大大提高了它的使用价值。

这本词典中不仅包含了同义词组，还包含了一定数量的同类词，即一些具有相关意义的词组。为了能更好地将其使用在中文信息处理中，哈尔滨工业大学信息检索研究室根据众多词语相关的资源对《同义词词林》进行完善，完成了《哈尔滨工业大学信息检索研究室同义词词林扩展版》，它去除了原版中14 706个罕用词和非常用词，最终包含77 343条

词语,包含较原版而言更丰富的语义信息。表 9-2 列出了《同义词词林》扩展前后的比较。

表 9-2　《同义词词林》扩展前后的比较

词典特征	扩展前	扩展后	词典特征	扩展前	扩展后
词条总数/个	53 895	77 343	小类数/个	1428	1400
大类数/个	12	12	层次数/层	3	5
中类数/个	94	97	编码长度	4	8

在《哈尔滨工业大学信息检索研究室同义词词林扩展版》中,是以表 9-3 所示方式存储的。它的编码位是按照从左到右的顺序排列的。第一位表示词所在的大类,第二位表示词所在的中类,第三位和第四位表示词所在的小类,第五位表示词群,第六位和第七位为原子词群,第八位的标志有 3 种,分别是"＝""＃"和"@"。其中,"＝"代表这组词是同义词;"＃"代表这组词是同一类词,它们属于相关词组,但是并非同义词;"@"代表这组词是独立的词,它在词库中既没有同义词,也没有相关词,见表 9-3。

表 9-3　同义词词林存储方式

词类编码	词组信息
Aa01A01＝	人物 人士 人氏 人选
Di09D49＃	报道组 采访组 摄制组
Bc03B02@	瓶颈

不同级别的分类结果可以为自然语言处理提供不同的服务。可以将同义词组分为 3 组,分别是完全可替换词组(语义完全相等的同义词组)、不完全可替换词组(部分语义相等的同义词组)和歧义词组(存在部分语义不相等的同义词组),并以此生成新的词库。现根据本章的研究特点对其进行相关的改动,得到本实验使用的中文同义词词库,具体构建步骤如下。

(1) 以《哈尔滨工业大学信息检索研究室同义词词林扩展版》为基础,取出其中的同义词组,即第八位为"＝"的词组。

(2) 将中华人民共和国教育部国家语言文字工作委员会分别于 2001 年和 2002 年发布的两批异形词表加入词库,并删除重复出现的同义词。

(3) 根据现代汉语词语的词频[174]统计删除生僻的同义词。

(4) 使用哈尔滨工业大学信息检索研究中心语言技术平台进行分词识别,同时删除在已有词库中不能正确识别的词语。

(5) 删除同义词组中所有为单字的同义词。

(6) 删除词库中同义词个数为 1 的同义词组。

2. 同义词词库的编码

文本文档的自身冗余较图像、音频等多媒体文件少得多,在传统的同义词替换算法中,简单的用"1"代表替换,用"0"代表不替换,其隐藏容量为 1 比特/词,隐藏算法本身对替换词也有要求,显然嵌入容量过少。我们期望找到一种能够提高隐藏容量的编码方式。

最简单的二进制编码方式是等长编码，但是这种编码方式会造成一定编码效率的损失。本章选择不等长编码方式，不但可以增加嵌入容量，还提高了编码率。采用不等长编码时，特别要注意避免译码的二义性或多义性。也就是说，在对一个字符集进行不等长编码时，要求任何一个字符的编码都不能是其他字符编码的前缀（即无前缀编码），这样在接收端就不会因歧义而翻译出错误的信息。为了使不等长编码成为无前缀编码，可以利用二叉树实现，具体方法见算法 9.1。

算法 9.1 同义词词库编码算法。

(1) 获取某一组同义词组中同义词的个数，记为 n。

(2) 构建具有 n 个叶子结点的编码二叉树。

① 建立二叉树的根结点，赋权值为 n。

② 建立该结点的左子结点，赋权值为$\lceil n \rceil$。

③ 建立该结点的右子结点，赋权值为$\lfloor n \rfloor$。

④ 重复②和③，直到二叉树的所有叶子结点的权值均为 1。

(3) 将得到的二叉树的所有左分支编码为“1”，所有右分支编码为“0”，以从根结点到叶子结点的路径上分支编码组成的码串作为该叶子结点的编码。

(4) 将得到的各个叶子结点的编码存入长度为 n 的数据结构中，用来保存各个同义词。

以“旅馆”为例，它在同义词词库中的同义词组为：“旅馆 旅社 客栈 招待所 宾馆 旅店”，根据同义词词库的编码算法，这是一个具有 6 个结点的编码二叉树，如图 9-1 所示。

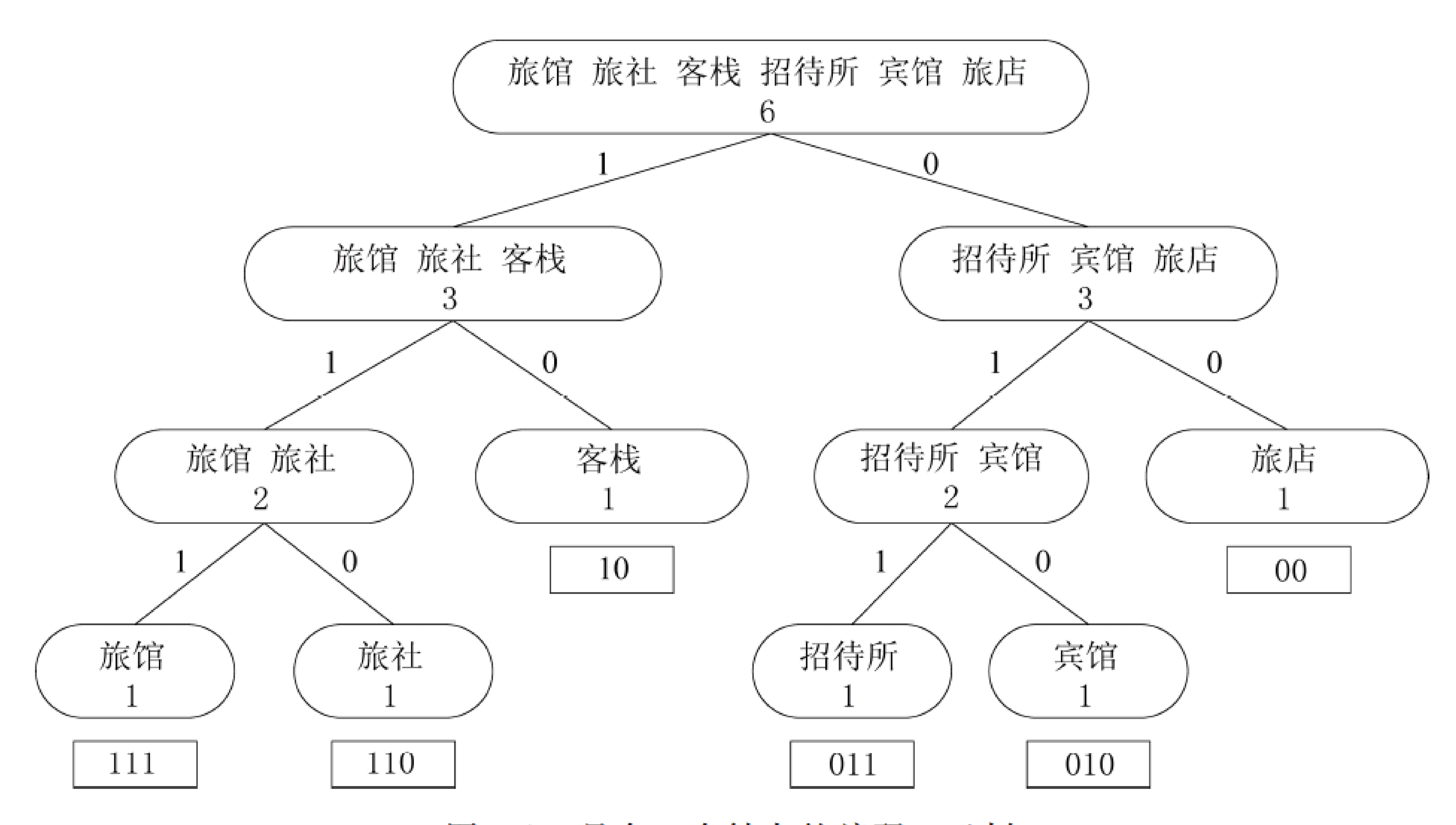


图 9-1 具有 6 个结点的编码二叉树

可以看到，编码二叉树各叶子结点的层次数之差为 1 或 0，利用从根结点到叶子结点的路径分支编码时，同一组同义词中词语的编码长度差也是 1 或 0。这样，在嵌入秘密信息时，平均嵌入容量为 $\log_2 n$ 比特/词，其中 n 为同义词组的个数，这样就克服了一个同义词只能编码一个比特位的缺点，提高了系统的隐藏容量。

9.3　基于同义词替换的信息隐藏

9.3.1　基于同义词替换的信息隐藏算法

基于中文同义词替换的隐藏算法主要包括以下 5 个部分，如图 9-2 所示。

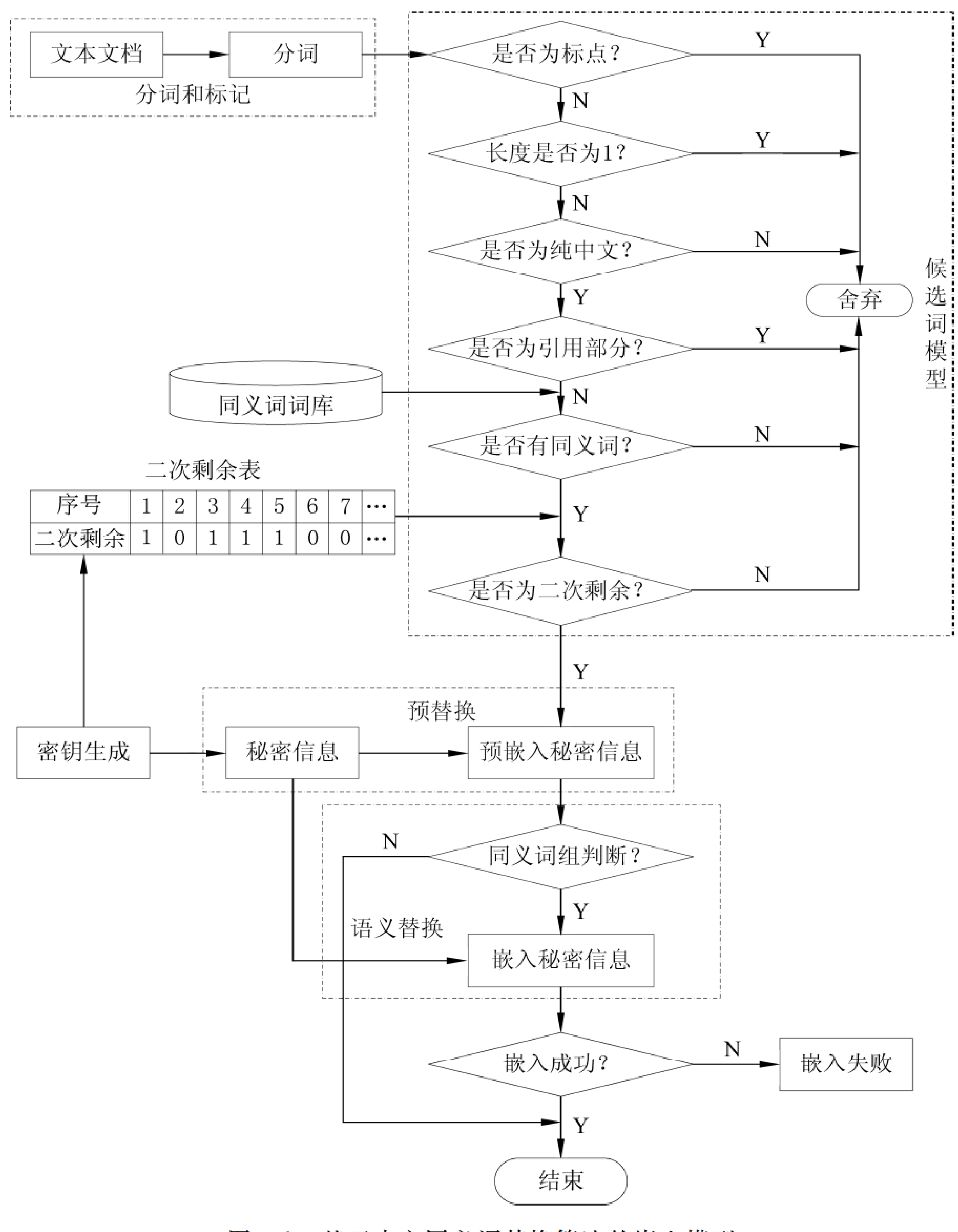


图 9-2　基于中文同义词替换算法的嵌入模型

(1) 密钥生成：嵌入秘密信息使用的密钥是由嵌入密钥和二次剩余密钥组成的。首先，利用嵌入密钥对秘密信息进行编码，将其转换为比特串；然后利用二次剩余密钥生成

一个二次剩余表，这个表格主要是帮助我们选择待替换的候选词，根据二次剩余密钥，如果一个数为二次剩余密钥的二次剩余(表示为1)，则将这个数对应的词作为候选词，反之相反。

(2) 分词和标记：分词和标记在中文同义词替换算法中是必需的。一个好的分词系统对隐藏算法来说尤为重要，此次选取的是哈尔滨工业大学信息检索研究中心语言技术平台，该平台拥有丰富的中文词库以及多种语言处理模块，可以达到理想的分词效果。

(3) 候选词模型：在分词和标记之后便可对其中的词进行替换，从而嵌入秘密信息。候选词就是被选中要进行替换的词。不能盲目选择候选词，必须考虑很多因素，过滤掉一些不合适的词语，如图9-2中的候选词模型所示。下面对过滤规则进行简单描述。

① 标点符号：标点符号是固定的且很难改变，在本次方案中不考虑标点符号。

② 长度为1的分词：经分词系统处理的句子中，长度为1的分词一般都是代词、介词或者连词等，这些词很难或者不可能被替换，因此也不予考虑这些词。

③ 非纯中文的词：本实验的研究内容是针对中文载体的，由于在分词系统中不能识别非中文的词，如英语、日语或者一些中英混合词(如“T恤”)等，因此本课题中不考虑如何处理这些词的问题。

④ 引用部分：通常在文本中会出现一些引用部分，如书名号，书名号之间的部分往往来自一些特定用语，如果修改这部分内容，会引起攻击者的注意，因此不考虑这些词的处理问题。

⑤ 没有同义词的分词：没有同义词的分词是不能嵌入秘密信息的，这些词必须省去。

⑥ 虽然一些分词有同义词，但是它不在二次剩余表中。也就是说，这些分词是二次剩余密钥的非二次剩余，不进行替换，这些词也必须被删去。

(4) 预替换：通过候选词模型可以嵌入秘密信息，但是考虑到经过同义词替换后，由于上下文语境的不同可能会破坏语义的一致性，在此作预替换处理。文献[174]提出了一种同义词组判别算法，有效解决了语义一致性的问题。

(5) 语义替换：这部分将转化为比特串的秘密信息嵌入隐密载体，即文本文档中。在预替换中，利用同义词判别算法进行判断，判断结果正确时即可通过“与或”运算嵌入秘密信息；否则不做替换。

在介绍具体算法前，首先进行如下定义。

C：载体文本；M：秘密信息；S：嵌入秘密信息后的文本；K：密钥；D：同义词词库。

算法 9.2 若基于同义词替换的信息隐藏算法。

① 将秘密信息 M 编码成二进制比特串，再根据密钥 K，令 $K'=K^{-1}$，采用3DES(三重数据加密算法的通称，相当于对每个数据块应用3次DES加密算法)算法[176,177]对秘密信息 M 进行加密，此时 $M'=E(K,D(K',E(K,E)))$。

② 对载体文本 C 进行分词。

③ 利用密钥 K 生成二次剩余密钥 K_1。

④ 遍历 C 中的每一个分词，根据同义词词库 D 和 K_1，利用候选词模型判断该分词是否为候选词，若是，则转⑤，否则转⑦。

⑤ 根据候选词所在的同义词词组进行预替换，利用同义词判别算法进行判别。

⑥ 若判别结果为真，则根据同义词词组的编码嵌入秘密信息；若判别结果为假，则转⑦。

⑦ 重复执行④～⑥，直到整个 M' 全部嵌入完成，生成替换后的文档 S，否则嵌入失败。

9.3.2 基于同义词替换的信息提取算法

秘密信息的提取算法是嵌入算法的逆过程。在提取中不需要原始文本，属于盲提取。它与嵌入算法不同的是，提取秘密信息时不用进行预替换，也不需要对同义词进行替换，而是需要将候选词和编码后的同义词组进行对比，从而提取出秘密信息的比特串。

算法 9.3 基于同义词替换的信息提取算法。

① 对嵌入秘密信息的文本 S 进行分词。

② 根据密钥 K 生成二次剩余密钥 K_1。

③ 遍历 S 中的每一个分词，根据同义词词库 D 和 K_1，利用候选词模型，判断该分词是否为候选词，若是，则将其与编码后的同义词组进行对比，恢复出秘密信息的二进制比特串 M'，否则跳过该词继续处理下一分词。

④ 重复执行③，直到遍历完 S 中的每一个词。

⑤ 根据密钥 K，令 $K'=K^{-1}$，采用 3DES 解密，得到秘密信息 M，$M=D(K,E(K',D(K,M')))$。

9.3.3 多载体模型中的中文同义词替换算法

在被动攻击的情形下，多载体模型较单载体模型而言，具有较高的安全性。在多载体模型中使用中文同义词替换算法较单载体模型更复杂，最重要的是需要知道各个载体和秘密信息之间的对应关系。本章利用条件转移概率 P 将分组后的秘密信息嵌入不同的载体中，以确定载体和秘密信息之间的对应关系，具体表示为

$$diag((c_1,c_2,\cdots,c_n)\otimes((m_1,m_2,\cdots,m_n)P_n)')=(s_1,s_2,\cdots,s_n) \tag{9-1}$$

式(9-1)中的 P_n 为条件转移概率，它是一个 n 阶方阵，它的每一行每一列中只有一个元素为 1，其余都为 0，$\otimes$表示嵌入运算，例如：

$$diag\left((c_1,c_2,c_3,c_4)\otimes\left((m_1,m_2,m_3,m_4)\begin{bmatrix}0&1&0&0\\0&0&0&1\\1&0&0&0\\0&0&1&0\end{bmatrix}\right)'\right)$$

$$=diag\left(\begin{bmatrix}c_1\otimes m_3&&&\\&c_2\otimes m_1&&\\&&c_3\otimes m_4&\\&&&c_4\otimes m_2\end{bmatrix}\right)$$

$$=(s_1,s_2,s_3,s_4) \tag{9-2}$$

式(9-2)表示在嵌入模型中共有 4 个载体，同时秘密信息被分为 4 组，根据条件转移

概率 P_4 将 m_1、m_2、m_3、m_4 分别嵌入 c_2、c_4、c_1、c_3 中。特别地，当 P_n 为单位矩阵时，多载体模型则退化为单载体模型。可以说，单载体模型是多载体模型的一种特殊情形。

条件转移概率 P_n 由密钥 K 和载体个数 n 共同决定。P_n 的计算方法见算法 9.4。

算法 9.4 P_n 的计算方法。

① 建立一个长度为 n 的数据结构，初始化为连续的自然数序列，即 $0\sim n-1$，如图 9-3 所示。

② 计算 $l(i)=h(K,n,i)=k^{n-i} \bmod n, i\in[1,n]$。

③ 将 $l(i)$ 的值与①中数据结构的值进行对比，并在相应位置存入 i 的值，若造成冲突，则将 i 的值存入其后第一个不为空的位置。

④ 根据图 9-3 生成的数据结构生成 P_n，P_n 的第 j 行第 i_j 列元素为 1，其余元素均为 0。

0	1	2	3	…	$n-1$

→

0	1	2	3	…	$n-1$
i_0	i_1	i_2	i_3	…	i_{n-1}

图 9-3 P_n 生成图

例如：求 $K=7, n=5$ 时的条件转移概率 P_5。

① 生成数据结构 0～4。

② 计算 $l(i)$。

$l(0)=h(7,5,0)=7^5 \bmod 5=2$;

$l(1)=h(7,5,1)=1$;

$l(2)=h(7,5,2)=3$;

$l(3)=h(7,5,3)=4$;

$l(4)=h(7,5,4)=2$;

③ 根据计算的 $l(i)$ 的值将其存入①生成的数据结构中，如图 9-4 所示。

i →	0	1	2	3	4
j →	4	1	0	2	3

图 9-4 P_5 生成图

④ 根据图 9-4 得到条件转移概率 P_5。P_5 的第 i 行第 j 列对应的位置元素均为 1，其余元素均为 0，则有

$$P_5=\begin{pmatrix}0&0&0&0&1\\0&1&0&0&0\\1&0&0&0&0\\0&0&1&0&0\\0&0&0&1&0\end{pmatrix}$$

经算法 9.4 得到 P_n，也就是说，得到了各个载体与秘密信息之间的对象关系，就可以按照这个对应关系嵌入秘密信息了。下面介绍多载体模型中的替换算法，如图 9-5 所示。

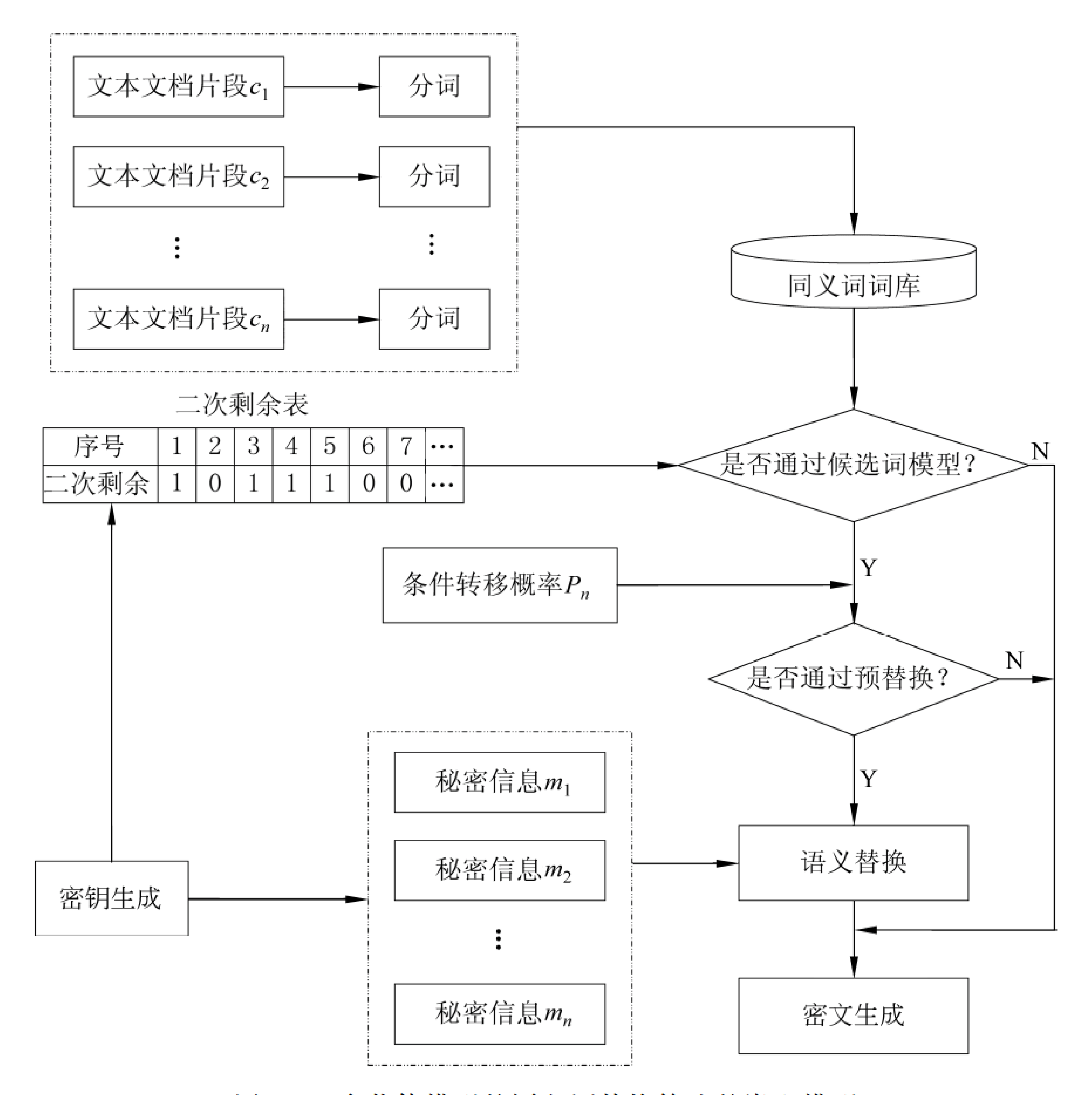


图 9-5　多载体模型的同义词替换算法的嵌入模型

与 9.3.1 节中介绍的同义词替换算法类似，多载体模型中的替换算法中同样包括密钥生成、分词和标记、候选词模型、预替换和语义替换五大部分。不同的是，这里的秘密信息被分为多个秘密信息块，与此同时，分词是对多个载体均进行分词，通过候选词模型的分词需经过条件转移概率 P_n 将秘密信息预替换到不同的载体中，此时如不影响上下文语境，则嵌入秘密信息，得到嵌入秘密信息的文档，具体算法如下。

算法 9.5　多载体模型中的中文同义词替换算法。

① 将秘密信息 M 编码成二进制比特串，再根据密钥 K，令 $K'=K^{-1}$，采用 3DES 算法对秘密信息 M 进行加密，此时 $M'=E(K,D(K',E(K,M)))$。

② 将 M' 分为 N 组，得到 m_i，$i\in[1, N]$。

③ 将载体 C 分为 N 组，得到 c_j，$j\in[1, N]$。

④ 根据密钥 K 和分组个数 N 计算条件转移概率 P_n，由 P_n 得出(m_i,c_j)并标记(i,j)的配对情况。

⑤ 利用密钥 K 生成二次剩余密钥 K_1。

⑥ 对 c_j 进行分词，遍历 c_j 中的每一个分词，根据同义词词库 D 和 K_1，利用候选词判

断其是否为候选词，若是，则进行预替换，否则转⑧。

⑦ 如果通过预替换，则根据同义词词组的编码嵌入 m_i，否则转⑧。

⑧ 将 j 加 1 转⑥，直到所有的 M' 嵌入完成，得到 s_j。

⑨ 根据 (i,j) 的配对情况得到序列 $(s_1,s_2,\cdots,s_n)$，即嵌入秘密信息的文档 S。

9.3.4 多载体模型中的中文同义词提取算法

多载体模型在提取秘密信息的过程中同样不需要原始文本，提取时仍然是将候选词和编码后的同义词词组进行对比，从而提取出秘密信息的比特串，但是这里需要知道载体的个数 N，并根据载体个数 N 和密钥 K 确定载体与秘密信息之间的对应关系，具体算法如下。

算法 9.6 多载体模型中的中文同义词提取算法。

① 将 S 分为 N 组，得到 s_j，$j\in[1, N]$。

② 对 s_j 进行分词。

③ 利用密钥 K 生成二次剩余密钥 K_1。

④ 遍历 s_j 中的每一个分词，根据同义词词库 D 和 K_1，利用候选词模型，判断该分词是否为候选词，若是，则将其与编码后的同义词组进行对比，恢复出秘密信息的二进制比特串 m_i，否则跳过该词继续处理下一分词。

⑤ 根据密钥 K 和分组个数 N 计算条件转移概率 P_n，由 P_n 得出 (m_i,s_j) 并标记 (i,j) 的配对情况。

⑥ 将 j 加 1 转④，直到遍历完所有的 s_j。

⑦ 根据 (i,j) 的配对情况恢复出正确的秘密信息序列 $M'=(m_1,m_2,\cdots,m_N)$。

⑧ 根据密钥 K，令 $K'=K^{-1}$，对 M' 采用 3DES 解密，得到秘密信息的二进制比特串 M，$M=D(K,E(K',D(K,M')))$，对 M 编码得到秘密信息。

9.4 算法的性能比较

在本章前面几节的讨论中，由于考虑了上下文语境，基于单载体的同义词算法已经基本消除了可能产生歧义的同义词替换，这样使替换后的文本仍然是一个语法正确且语义连贯的文档。

在多载体模型的中文同义词替换算法中，在保证语义连贯的基础上，根据各个载体和分块之后秘密信息间的不同对应关系嵌入秘密信息，提高了系统的安全性。

具体实验如图 9-6 所示，其中图 9-6(a)为原始文本，图 9-6(b)、(c)分别为在单载体隐藏模型和多载体隐藏模型中进行中文同义词替换后的截图。

为了对比改进前后两种算法的同义词替换结果，分别用两种模型中的算法对约 1000 个文本进行了实验，实验结果见表 9-4，其中嵌入容量＝替换字数/载体字数；准确度＝准确替换词数/替换词数。



原始文本.txt - 记事本

　　白日的喧嚣还未退去，窗帘的外面，已经是漫无边际的黑。夜的帷幕像沁开的墨汁一般，铺染了所有的空间。虽然还有无数的烦躁依旧抗争着这自然的落幕，但那份夜的宁静，却是不请自来，让我们被生活污染的心灵，慢慢地趋于宁静。这样的夏夜，多半是多情而又迷人的，天上有着挨挨挤挤的星子，轻声呢喃着情话，一钩弯弯的月，勾起无尽的思念。偶尔有几只山鸟被月光惊醒，用轻盈的翅划过蓝蓝的天宇，那清脆的鸣叫打破了夜的宁静，也惊醒了无数游子思乡的梦。斑斑驳驳的，透过树叶缝隙而来的光，在地面上，像一幅幅的水墨画。山间宁静的夜，偶尔也会被风声敲碎，听那漂泊而至的风，轻轻地，在不远的林海，泛起一阵又一阵细小的波浪。在这样美丽的夜，我最期待的却是不经意间响起的喧嚣的虫鸣。在这样宁静而又柔软的夜里，曾经独坐窗前的我，最爱的是捧一杯酽茶，静静地坐着，看着水汽从手上上升，逐渐蔓延开来。面对茫茫的黑夜，编织着一个又一个属于自己的童话。累了的时候，就闭上眼睛，让思绪停顿下来，静静地等待，窗外的虫鸣响起。

(a) 原始文本



单载体隐藏.txt - 记事本

　　白日的吵闹还未退去，窗帘的外头，早已是漫无边际的黑。夜的帷幕像沁开的墨汁一般，铺染了全部的长空。虽然还有无数的烦乱兀自勇斗着这原始的剧终，但那份夜的静穆，却是不请自来，让我们被小日子污染的心灵，逐渐趋于幽僻。这般的夏夜，过半是脉脉含情而又可喜的，天空有着挨挨挤挤的星子，轻声呢喃着情话，一钩弯弯的月，勾起尽头的怀念。偶然有几只山鸟被月华惊醒，用轻盈的翅划过蓝蓝的苍穹，那清脆的鸣叫打破了夜的静静，也惊醒了众多游子思乡的梦。薄薄驳驳的，透过叶子缝隙而来的光，在地方上，像一幅幅的水墨画。山间冷静的夜，有时候也会被风声敲碎，听那浮生而至的风，轻度，在不远的密林，泛起一阵又一阵细微的浪花。在这样美丽的夜，我最愿意的却是忽视间响起的喧嚣的虫鸣。在这样宁静而又软绵绵的夜里，久已独坐窗前的我，最爱的是捧一杯酽茶，静静地坐着，看着水汽从目前上升，逐渐蔓延开来。面对着茫茫的黑夜，编织着一个又一个属于自己的童话。累了的时候，就闭上眼睛，让思绪停顿下来，静静地等待，窗外的虫鸣响起。

(b) 单载体隐藏



多载体隐藏.txt - 记事本

　　白日的吵闹还未退去，窗帘的外头，早已是漫无边际的黑。夜的帷幕像沁开的墨汁一般，铺染了全部的长空。虽然还有无数的烦乱依然抗争着这天然的落幕，但那份夜的恬静，却是不请自来，让我们被生活污染的心灵，渐渐趋于宁静。这样的夏夜，过半是脉脉含情而又动人的，天空有着挨挨挤挤的星子，轻声呢喃着情话，一钩弯弯的月，勾起无尽的惦念。间或有几只山鸟被月色惊醒，用轻盈的翅划过蓝蓝的苍穹，那清脆的鸣叫冲破了夜的恬静，也惊醒了众多游子思乡的梦。斑斑驳驳的，透过叶子缝隙而来的光，在地面上，像一幅幅的水墨画。山间宁静的夜，有时候也会被风声敲碎，听那漂泊而至的风，轻轻的，在不远的树林，泛起一阵又一阵小小的浪花。在这样美丽的夜，我最盼望的却是不经意间响起的喧嚣的虫鸣。在这样恬静而又柔软的夜里，早已独坐窗前的我，最爱的是捧一杯酽茶，静静地坐着，看着水汽从手上上升，逐渐迷漫开来。面对着茫茫的黑夜，编织着一个又一个属于自己的童话。累了的时候，就闭上眼睛，让思绪停顿下来，静静地期待，窗外的虫鸣响起。

(c) 多载体隐藏

图 9-6　具体实验

表 9-4　实验结果

类　　型	单载体隐藏	多载体隐藏	类　　型	单载体隐藏	多载体隐藏
载体字数	405	405	准确替换词数	70	78
同义词数	100	100	嵌入容量	48.4%	49.88%
替换字数	196	202	准确度	79.55%	85.71%
替换词数	88	91			

可以看出，多载体模型的嵌入容量提高了1.48%，替换的准确度提高了6.16%，有效提高了隐藏模型的隐蔽性和鲁棒性。

隐密通信篇

隐密通信篇以网络环境为背景，主要介绍如何利用信息隐藏技术解决数字内容的信息泄露问题，并针对手机App系统的个人隐私保护问题提出了新的思路，展示了最新的研究应用成果。这部分内容第10～12章讲述。其中，第10章介绍文本替换的隐藏系统；第11章介绍基于H.264视频压缩标准的隐密通信；第12章介绍基于移动终端的隐密系统开发。

第 10 章 文本替换的隐藏系统

摘要：所谓隐信道，就是在公开信道中构造出的一种进行隐藏通信的信道。该信道的存在仅为秘密通信的用户所知，而公开信道只是作为隐藏通信的掩护体。

本章介绍一种在互联网即时通信背景下的秘密信息隐蔽通信系统，目的是解决网络通信中敏感信息的保密传输问题。实例中，将通信信息的范围限制为中文文本，利用中文同义词替换的隐藏算法将秘密信息嵌入网络聊天会话中，从而使秘密信息安全地到达接收方。

10.1 系统的总体设计

在即时通信背景下嵌入秘密信息和通常的在文本中嵌入水印信息的概念并不相同。通常的嵌入水印的目的是保护和认证嵌入载体本身内容，而在隐蔽通信情况下，更重要的是秘密信息的保护问题，二者侧重点不同。另外，在即时通信过程中进行嵌入和提取时，收发双方需要密切合作，以解决通信的起始、结束、同步及校验等问题。

即时通信背景下的隐蔽通信系统的体系结构可以采用图 10-1 所示的伪客户端结构。

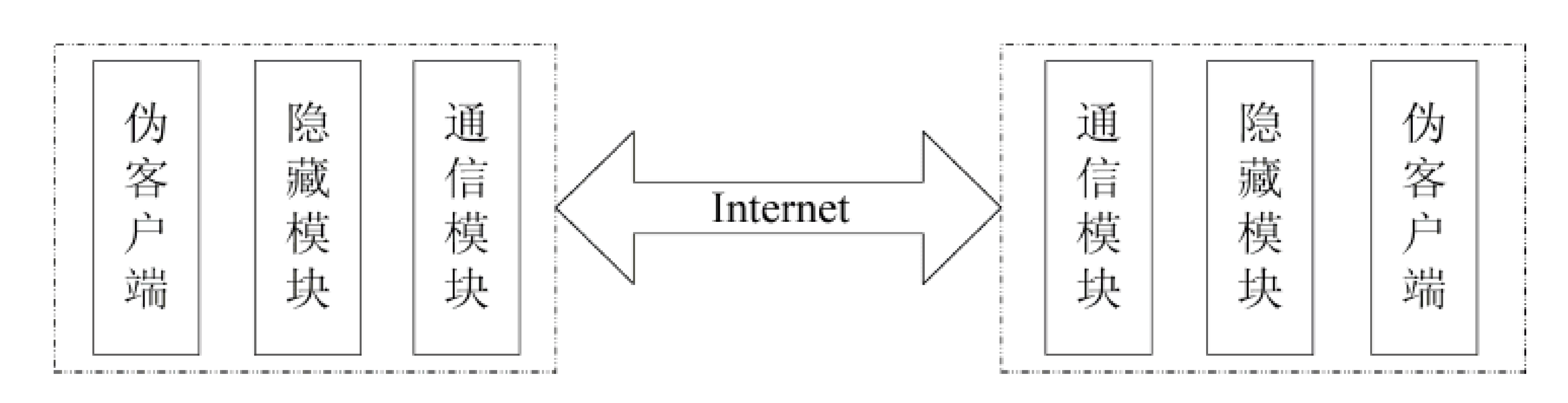


图 10-1　伪客户端结构

在伪客户端结构的体系中，抛弃了网络通信系统原有的客户端，编写新的客户端，这样可以无缝集成信息隐藏功能和网络通信功能。

本例中将涉及信息隐藏的各个模块嵌入在伪客户端的表面下。嵌入端以点对点通信一方的聊天语句作为单位载体，将秘密信息分块后通过密钥嵌入到不同的聊天语句中，并在公开的信道上发送；解析端则通过密钥从接收到的语句中提取秘密信息，此时不需要原始载体语句，即采用盲提取方式。

对于攻击者而言，在网络信道截获的含密语句表面上与普通聊天语句并没有差别，由于不知道原始载体语句的内容，所以无法察觉和获得秘密信息。系统总体设计框图如图 10-2 所示。

混合密钥包括对秘密信息进行编码加密的密钥 K_1、在隐藏时使用的隐藏密钥 K_2 和

同义词词组编码密钥 K_3。嵌入时，将需要秘密发送的消息经过编码、加密、分组等一系列操作形成一个二进制码串；网络通信双方在对话过程中生成聊天文本，通过中文同义词替换将秘密信息形成的二进制码串嵌入到聊天文本中得到含密文本；含密文本在公开信道上发送至接收方。提取端的操作与发送端完全相反，这里不再赘述。

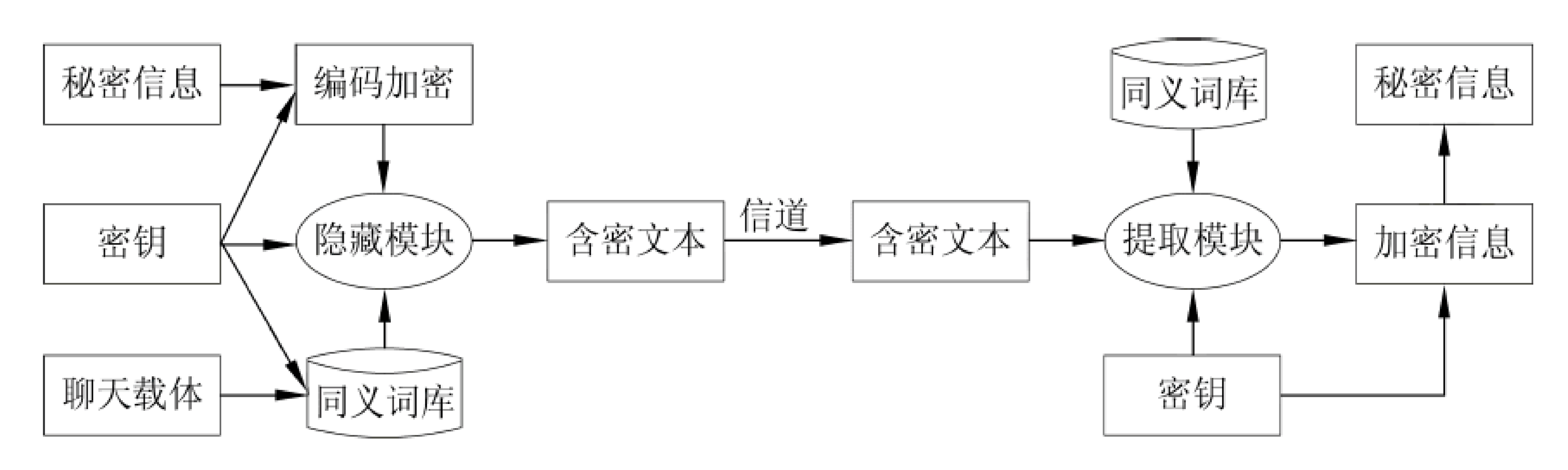


图 10-2 系统总体设计框图

10.2 详细设计

在即时通信背景下，通信双方希望在通信过程中嵌入秘密信息，基于网络聊天的特点，需要将秘密信息嵌入在多个文本载体中。下面介绍本系统的详细设计。

10.2.1 帧结构的设计

在数据通信中，数据链路层把网络层交下来的数据封装成帧(Framing)发送到链路上，以及把接收到的帧中的数据取出并上交给网络层。在处理过程中，一般都是将原始比特流封装成离散的帧，然后以帧为单位发送，并在帧内完成差错检测、同步等控制，如图 10-3 所示。

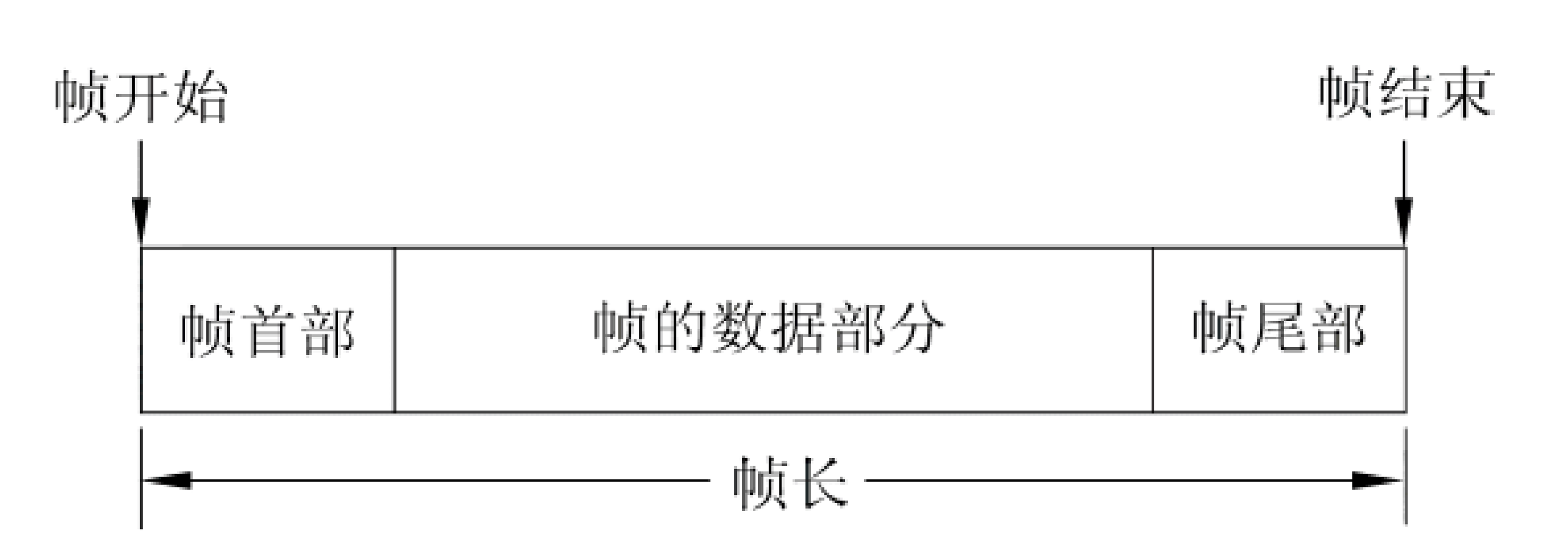


图 10-3 用帧首部和帧尾部封装成帧

封装成帧就是在一段数据的前后分别添加首部和尾部，这样就构成了一个帧。帧长等于数据部分的长度加上帧首部和帧尾部的长度，而首部和尾部的一个重要作用就是进行帧界定，它里面包含了许多必要的控制信息。而接收端在收到物理层上交的比特流后，就能根据首部和尾部的标记，从收到的比特流中识别帧的开始和结束，有效地解决了同步问题，如图 10-3 所示。

在隐蔽通信中，由于攻击者的存在，需要在应用层完成相应的操作，并以帧的形式在隐信道上传输。在本系统中，我们自行定义一种帧格式封装数据，并以这种帧格式为单位进行信息传输。将数据封装成帧时，需要进行帧界定，可作如图 10-4 所示的设定。



图 10-4　帧格式

（1）标志（FLAG）字段：以唯一的 01101010 在帧首部起界定作用，作为某一帧的起始标志。在双方通信的过程中，发送方不断向隐蔽信道发送消息，接收方不断从隐蔽信道提取发送方发出的比特流。当有秘密信息需要嵌入时，加上标志字段表示开始嵌入秘密信息。也就是说，在信道上传递消息时，当遇到标志字段时，认为一帧秘密信息开始传输，同样，接收端也是当遇到标志字段时，开始提取秘密信息。

这里存在一个问题，就是 01101010 这个码串可能出现在原始消息中的任何位置，这样就影响了标志字段的判断。为了解决这个问题，采用了位填充的方法，就是当发送方不需要或者没有准备好传递秘密信息时，此时不需要封装帧，在信息发送前对其进行预处理，每当出现连续 5 个 1 后，就将其下一位赋为 0，这样就有效避免了偶然的标志字段的出现。

（2）编号字段：也是帧首部的一部分，它是在一次通信中不同帧的唯一标识。编号字段一共有 8b，可以标识 256 个帧，这也是发送秘密信息的上限。当数据在传输中出现差错时，编号字段的作用更加明显。当某一帧发送失败或者错误时，发送方不需要重新发送所有信息，而是根据接收方反馈的帧编号选择性地重新发送。

（3）数据字段：即真正需要传送的信息。这里先对秘密信息进行加密，然后将加密后的秘密信息嵌入到载体文本中，最终得到的含密载体构成数据字段。

（4）校验字段：在现实的通信过程中都不会是理想的。也就是说，比特流在传输过程中可能会产生差错：“1”可能会变成“0”；而“0”也可能变成“1”。本方案采取循环冗余检验（Cyclic Redundancy Check，CRC）检错技术，在每帧尾部增加 16b 校验字段。本方案没有增加纠错比特，若发生检验错误，则采取重发机制处理。

（5）末尾帧格式：本方案中，每帧的长度为 160b，也就是说，当发现每帧的标志字段时，接下来的 160b 为一帧，但是最后一帧的数据字段长度有可能为 1～128，为了封装最后一帧，可以为它设定一个特殊的帧格式，如图 10-5 所示。

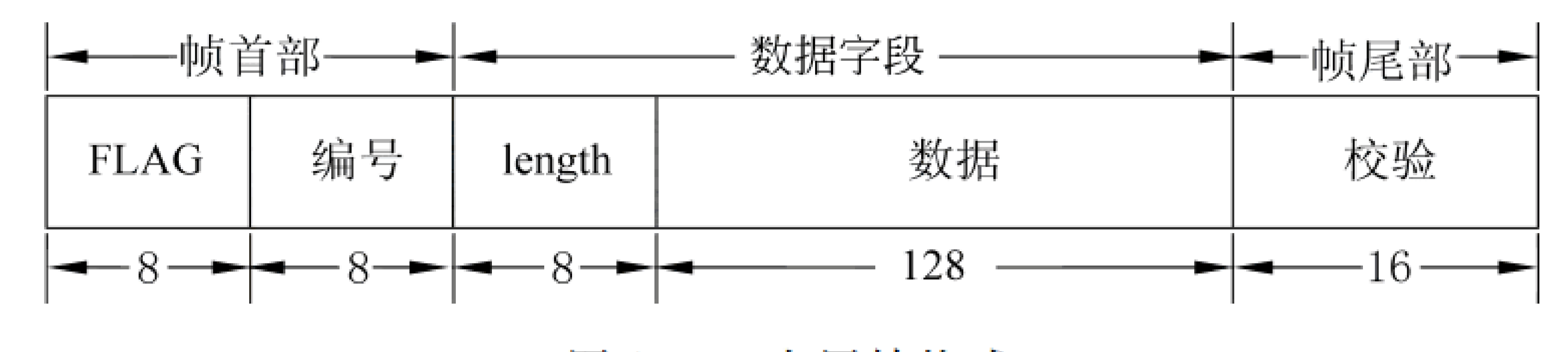


图 10-5　末尾帧格式

在末尾帧中，编号字段恒设为 10101010，在数据字段中加入数据长度，该字段记录了数据的长度（length），共 8b，根据数据长度字段确定末尾帧的长度。

10.2.2 差错检测

在信息传输过程中不可避免地会产生差错，我们在传输过程中把数据划分为帧，每一帧都加上冗余码，一帧接一帧地传送，然后在接收方逐帧进行差错检验。凡是接收端能接收到的帧，我们都能以非常接近 1 的概率认为这些帧在传输过程中没有产生差错。

前面已经提到，本方案中采用 CRC 差错检测技术，它可以有效做到对帧的无差错接收。若接收端因为有差错而没有接收到某些帧，可以根据帧的编号字段的编号确定哪些帧丢失，然后将丢失的帧重新发送，这样就可以达到“可靠传输”，即发送端发送什么，在接收端就能收到什么，如图 10-6 所示。

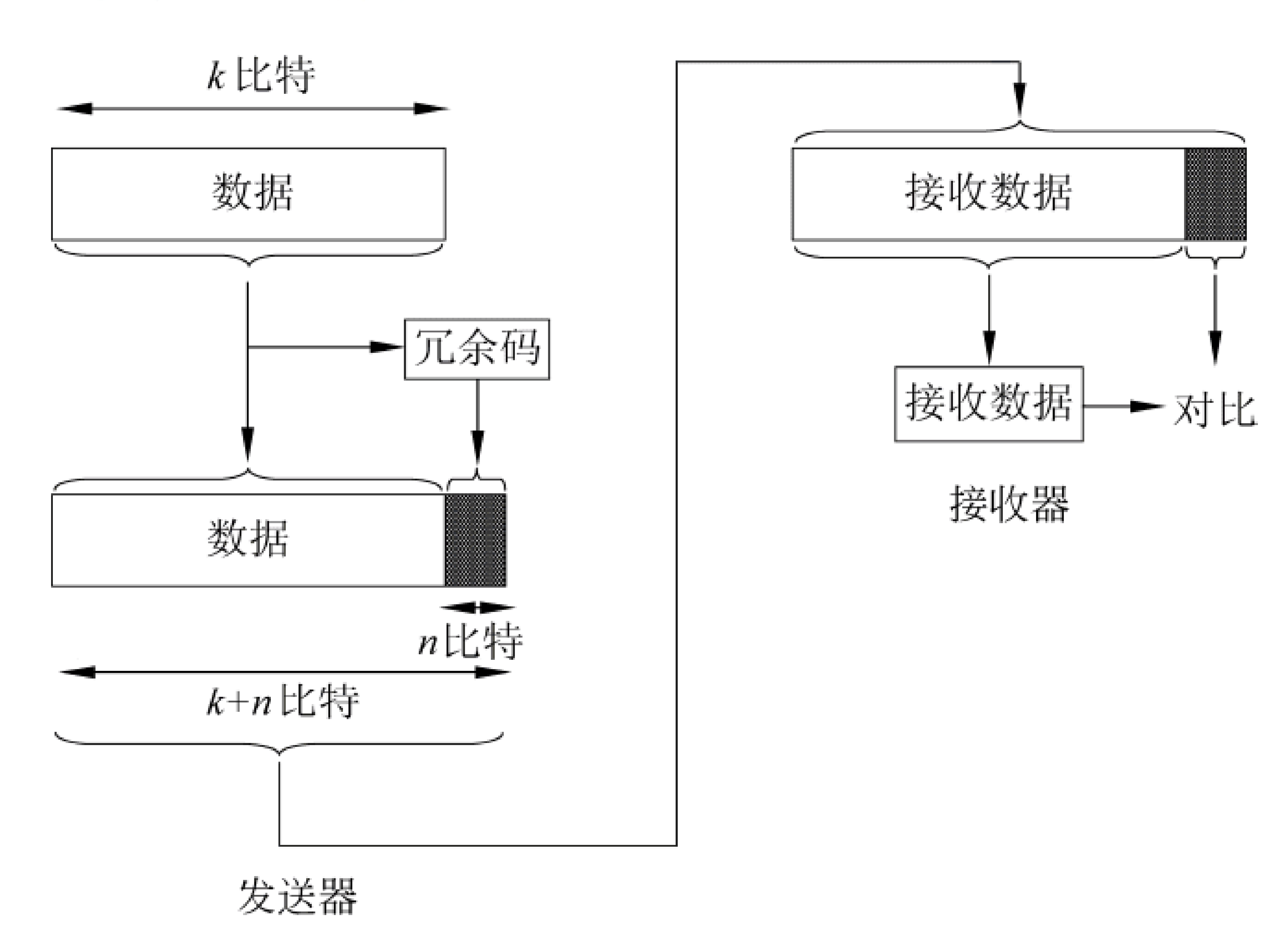


图 10-6 CRC 差错检测原理

CRC 差错检测原理如图 10-6 所示。在发送端，对于 k 比特的数据块 M，CRC 运算就是在数据块 M 的后面添加供差错检测用的 n 位冗余码，一起发送出去，一共发送 $(k+n)$ 位。这种为了进行检错而添加的冗余码称为帧检测序列(Frame Check Sequence，FCS)。这个比特序列要使最后得到的 $(k+n)$ 比特的帧可以被一些预先设定的数值整除，然后，接收器利用同样的数值对接收到的帧进行除法运算，如果其结果没有余数，则判定这个帧没有差错。本方案利用 CRC 差错检测技术将秘密信息和差错控制码进行绑定，作为嵌入信息共同添加到文本中，以达到在接收端可以检测偶发差错的目的。

在所要发送的数据后面增加 n 位冗余码，虽然增加了数据传输的开销，但却可以进行差错检测。当传输可能出现差错时，付出这种代价往往是值得的。

10.2.3 发送模块

发送模块主要是将秘密信息嵌入到用户正常的聊天语句中，然后通过隐信道发送给接收方。这部分主要包括以下两方面工作，在此首先进行如下定义。

C：载体文本；M：秘密信息；K：密钥；n：成帧个数；S：含密载体文本。

1. 秘密信息

利用隐信道发送秘密信息时，首先对秘密信息进行编码，然后利用密钥对其进行加密，最后对加密后的比特串封装成帧，此时需要注意封装后的最后一帧的格式与其他帧不同。

算法 10.1　帧封装算法。

① 将加密后的秘密信息 M' 以 128b 进行分组，即 $M'=m_1m_2\cdots m_n$，设 l 为 M' 的二进制编码长度，则 $n=\lceil l/128 \rceil$。

② 成帧，若 $n>256$，则成帧失败；若 $n\leqslant 256$，则首先将 m_1 至 m_{n-1} 作为数据段按照帧格式依次成帧，帧编号依次为 $0\sim n-2$，然后将 m_n 作为数据段按照末尾帧格式成帧，帧编号为 256(即编号字段为 10101010)。

2. 信息嵌入

信息嵌入主要是将封装成帧的秘密信息嵌入到正常的聊天语句中，然后发送给接收方，如图 10-7 所示。

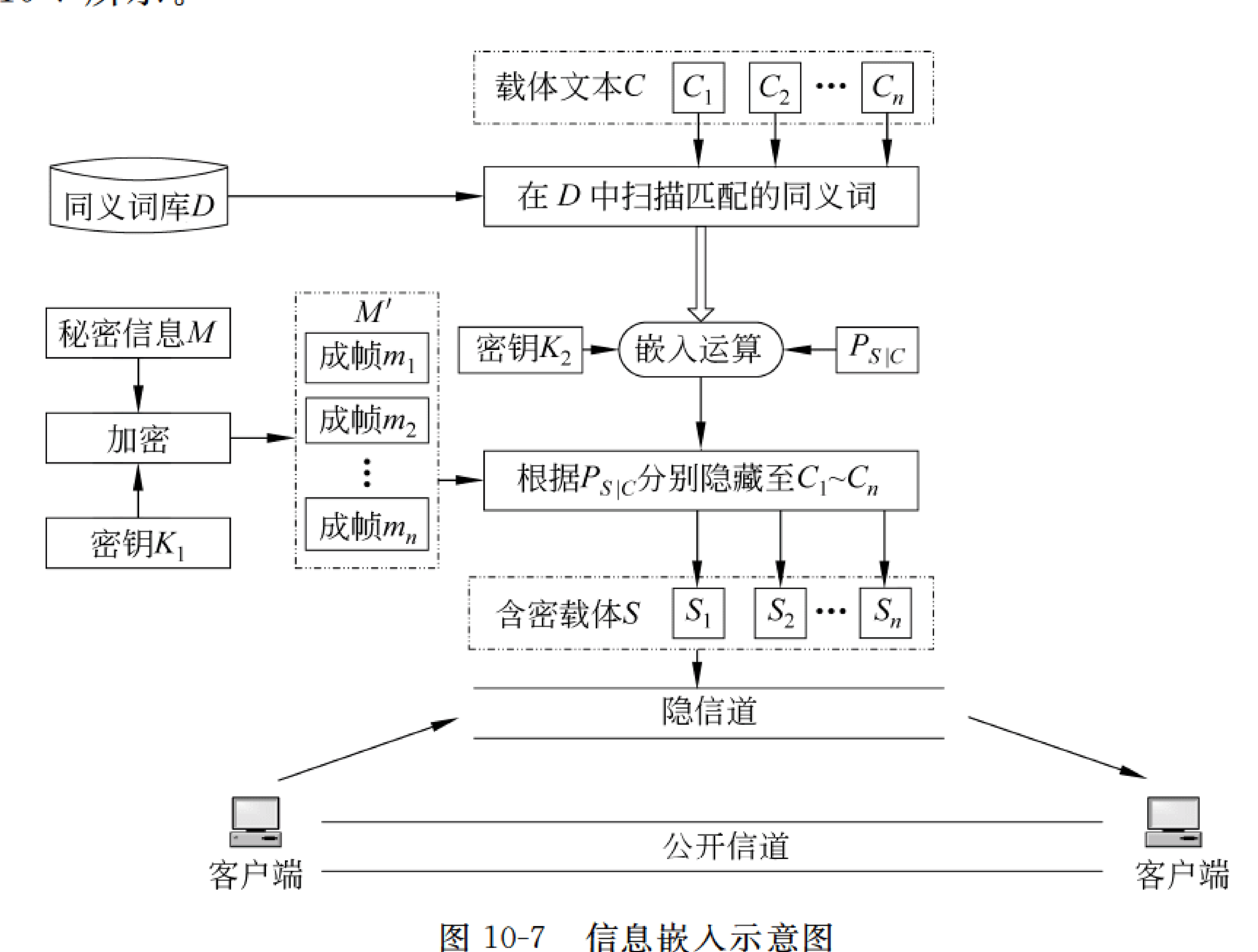


图 10-7　信息嵌入示意图

将用户的正常聊天语句(即载体文本 C)以每次发送的内容为单位进行处理，判断其是否符合替换条件，若符合，则根据条件转移概率 $P_{S|C}$，利用密钥 K_1 将已经封装成帧的秘密信息通过多载体模型中的中文同义词替换算法嵌入其中，并通过隐信道发送给接收方；若不符合就直接通过公开信道进行发送。具体流程如图 10-8 所示。

算法 10.2　发送端嵌入算法。

① 获取伪客户端聊天载体 $C=c_1c_2\cdots c_m$。

② 等待请求操作，若没有嵌入请求，则转⑩，若有嵌入请求，则转⑦。

③ 输入混合密钥 K。

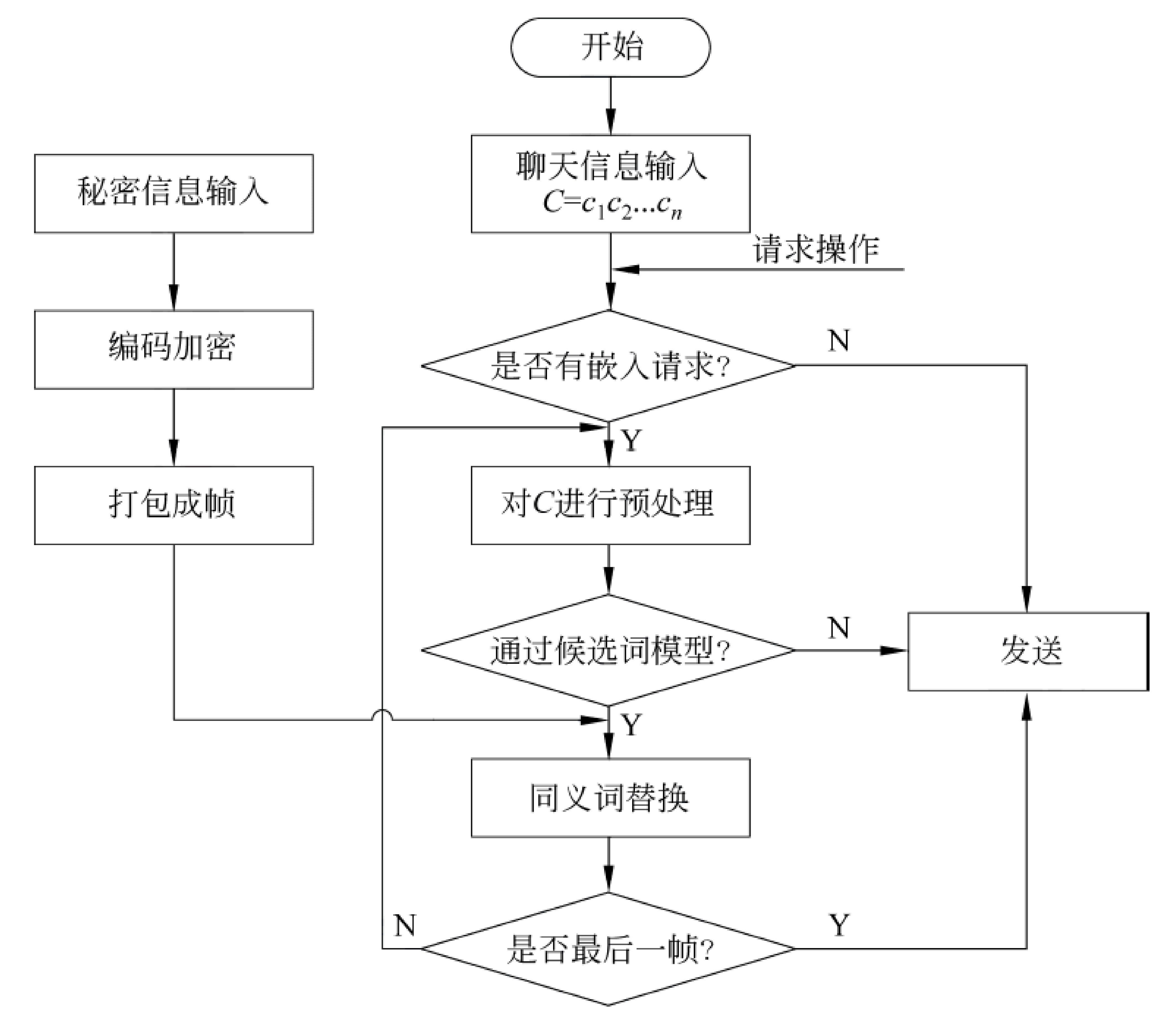


图 10-8　发送端流程图

④ 输入秘密信息，并取其 Unicode 编码得到二进制码串 M。

⑤ 根据密钥 K，令 $K'=K^{-1}$，采用 3DES 算法对秘密信息 M 进行加密，此时 $M'=E(K,D(K',E(K,M)))$。

⑥ 对 M'进行位填充，并封装成一组帧序列，共封装成 n 个帧。

⑦ 对聊天载体 $c_i(i\in[1,n],n\leqslant m)$进行预处理，若出现 5 个连续“1”，则将其下一位赋为“0”，否则不做处理。

⑧ 载体分析。若能通过候选词模型，则转⑨，否则转⑩。

⑨ 从混合密钥 K 中提取二次剩余密钥 K_1，同时根据 K 和帧的个数 n 计算条件转移概率 P_n，利用多载体模型中的中文同义词替换算法嵌入秘密信息。

⑩ 通过 Socket 发送消息。

⑪ 循环执行⑦～⑩，直到⑥中封装的所有帧均嵌入并发送完毕。

10.2.4　接收模块

与发送模块类似，接收模块同样包含两方面内容。首先是将封装成帧的秘密信息从经过替换的聊天语句中解析出来，然后从解析出来的一组帧中提取出秘密信息。在接收模块中需要用户输入与发送端相同的密钥，同样也需要与发送方相同的同义词库的支持。

1. 信息提取

根据接收到的聊天语句(即含密载体文本 S)和条件转移概率 $P_{S|C}$，利用密钥 K 将已经封装成帧的秘密信息提取出来。具体流程如图 10-9 所示。

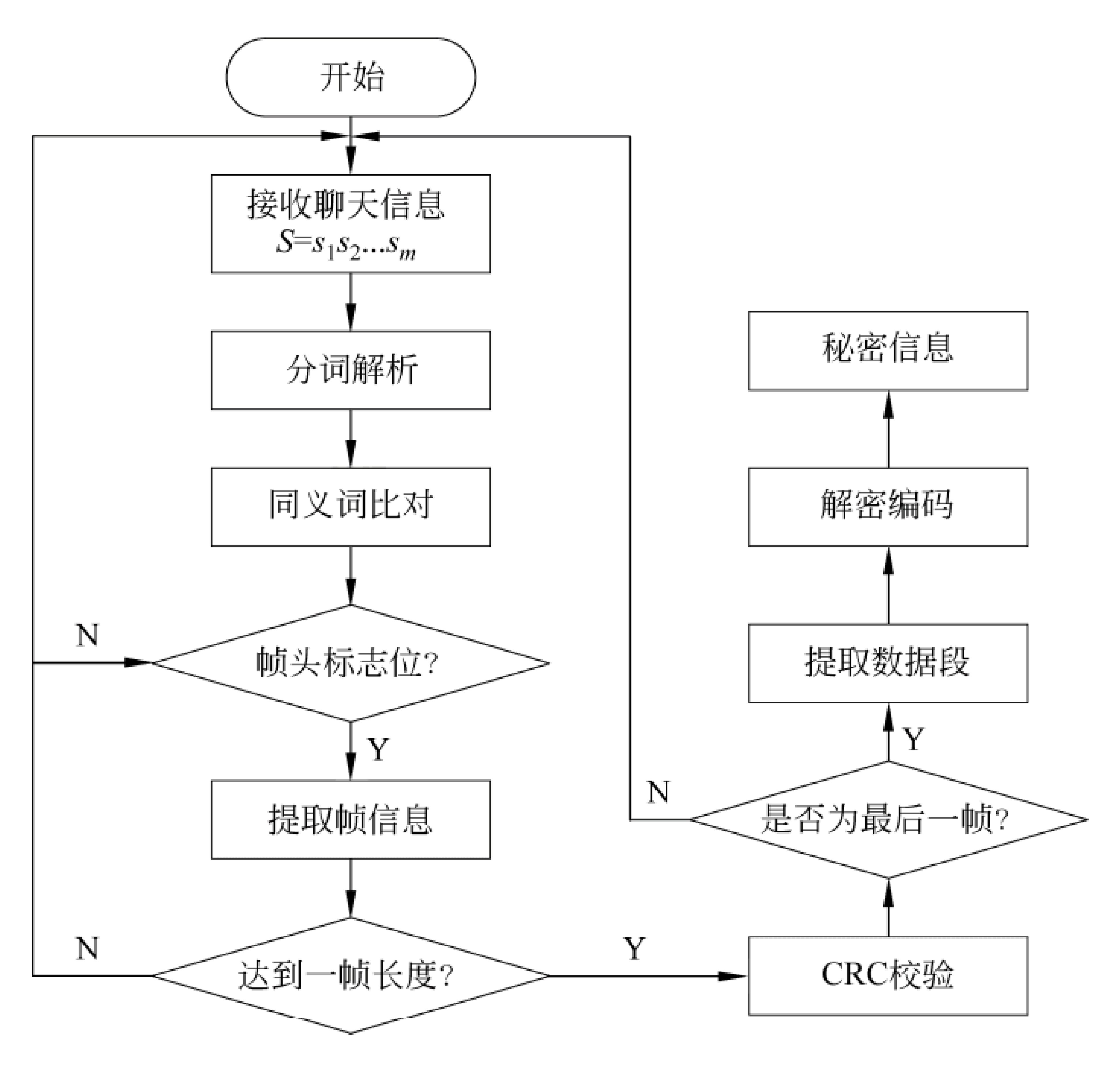


图 10-9 接收端流程图

首先对用户接收到的聊天语句进行分词解析，通过同义词比对找出封装成帧的信息的帧头标志位，提取帧信息，通过 CRC 校验后得到一组帧序列，然后从这组帧序列中提取出数据字段，再通过解密及编码恢复出秘密信息。

算法 10.3 接收端提取算法。

① 通过 Socket 接收伪客户端聊天语句 $S=s_1s_2\cdots s_m$。

② 输入混合密钥 K。

③ 从混合密钥 K 中提取二次剩余密钥 K_1。

④ 根据 K_1，对比同义词编码提取隐蔽信道信息。

⑤ 若出现帧起始标志，则启动计数器，$n=0$，否则转④。

⑥ 接收帧序号，判断是否为最后一帧，若不是，则将计数器 n 加 1，转④。

若是最后一帧，则转⑦，至此共提取出 n 个帧序列。

⑦ 对接收到的每一帧进行 CRC 校验。

⑧ 提取出所有帧的数据段，根据密钥 K 和帧的个数 n 计算条件转移概率 P_n，利用多载体模型中的中文同义词提取算法提取二进制串 M'。

⑨ 根据密钥 K，令 $K'=K^{-1}$，对二进制串 M' 采用 3DES 解密，得到秘密信息 M，$M=D(K,E(K',D(K,M')))$，然后将 M 按照 Unicode 编码得到秘密信息。

2. 帧解析

帧解析是指根据各个封装帧中的数据位组成的比特串，去掉其额外加入的比特位，得到实际的数据信息。解析时同样需要注意最后一帧的帧格式与其他帧格式的不同。

算法 10.4 帧解析算法。

① 从隐信道中提取秘密信息的比特串。

② 发现 FLAG 标志(01101010)后,若它不是最后一帧(FLAG 后的连续 8 位不是二进制 1101010),则连续接收 160b 数据(包括帧首部和帧尾部);若它是最后一帧(FLAG 后的连续 8 位是二进制 10101010),则根据末尾帧格式连续接收(length+40)b 数据(包括帧首部和帧尾部)。

③ 对接收到的帧进行 CRC 校验。

④ 分别从 n 个帧中提取数据段 $m_1, m_2, \cdots, m_n$ 组成加密后的秘密信息 M'。

10.3 系统实现

10.3.1 实验环境

以 Windows XP 操作系统为工作平台,使用 Visual C++ 6.0 进行系统的编译/汇编,开发语言为C++。

10.3.2 具体实现

在具体实现中选用基于客户(Client)/服务器(Server)体系结构的系统,减少网络瓶颈,提高数据传输效率,使用过程安全快速。系统中主要包括服务器端和客户端两部分。

1. 服务器端

进入服务器端系统时,需设置通信端口号,默认为 8888,并单击“启动”按钮,运行服务器端系统,如图 10-10 所示。服务器运行后,客户端就可以正常工作了。



图 10-10　服务器端

2. 客户端

本书之前提出的基于同义词替换的信息隐藏算法和隐蔽通信方案将在这部分实现。首先需有用户登录客户端，如图 10-11 所示。登录后会显示当前在线用户列表，如图 10-12 所示。



图 10-11　客户端登录



图 10-12　在线用户列表

通信双方通信时，首先需选择是“普通消息”，还是“隐藏消息”，如图 10-13 所示。普通



图 10-13　对话窗口

聊天就是正常的网络通信，此时没有秘密信息发送，因此不需要嵌入秘密信息；隐藏消息是指当有秘密信息发送时，需要嵌入秘密信息的消息，此时需要输入密钥和秘密信息，如图 10-14 所示。单击“初始化”按钮，系统将秘密信息封装成帧，用户输入聊天信息后，单击“开始嵌入帧”按钮，系统将把秘密信息嵌入到聊天载体中，这样就将秘密信息通过聊天载体发送给接收方，同时，帧嵌入进度条显示了秘密信息当前嵌入的容量。



图 10-14　嵌入/提取窗口

接收方接收到对方发来的信息时，输入提取密钥，这里的提取密钥和嵌入密钥是相同的，然后单击“初始化”按钮，就可以提取消息了，此时系统会提取出聊天载体中嵌入的帧信息，根据帧提取进度条的提示，当帧提取完毕时，就可以通过单击“解密”按钮得到秘密信息。

第 11 章 基于 H.264 视频压缩标准的隐密通信

视频因为其内容复杂，为隐密通信提供了丰富的掩饰体。另外，因为其容量大，因此大量的数据隐密通信提供了可能。本章基于 H.264 视频压缩编码标准，讨论了结合压缩、量化以及隐密的融合性视频隐密通信技术。

11.1 H.264 压缩编码简介

H.264 视频编码标准采用"回归基本"的简洁设计，获得比 H.263 好得多的压缩性能；加强了对各种信道的适应能力，采用"网络友好"的结构和语法，有利于对误码和丢包的处理；应用目标范围较宽，以满足不同速率、不同解析度以及不同传输（存储）场合的需求，如统一的 VLC 符号编码，高精度、多模式的位移估计，基于 4×4 块的整数变换，分层的编码语法等。这些措施使得 H.264 算法具有很高的编码效率，在相同的重建图像质量下，能够比 H.263 节约 50%左右的码率。H.264 的码流结构网络适应性强，增加了差错恢复能力，能够很好地适应 IP 和无线网络的应用。

11.2 帧内预测编码

帧内预测[178-180]编码流程如图 11-1 所示，是指利用当前帧中已重建宏块的编码信息对当前宏块进行预测的一种编码方式。利用当前编码块的相邻像素直接对当前块的每个像素值做预测，以消除空间冗余。在 H.264 帧内预测中，色度信息和亮度信息是分开预测的，并且各自具有多种预测模式。预测时需要采用特定的代价计算方法选择最佳预测模式，求得当前块的估计值。

在 H.264 中，帧内亮度预测[178]分为帧内 4×4 亮度预测和帧内 16×16 亮度预测两种模式，色度为帧内 8×8 色度预测。其中帧内 4×4 亮度预测有 9 种预测模式，主要用在细节较多的区域，而帧内 16×16 亮度预测有 4 种预测模式，主要用在图像中比较平坦的地方。帧内 8×8 色度预测和帧内 16×16 亮度预测较相似，有 4 种预测模式。

11.2.1 帧内 4×4 亮度预测

帧内 4×4 亮度预测是以一个 4×4 数据块为基本预测单元，利用左边和上边相邻块

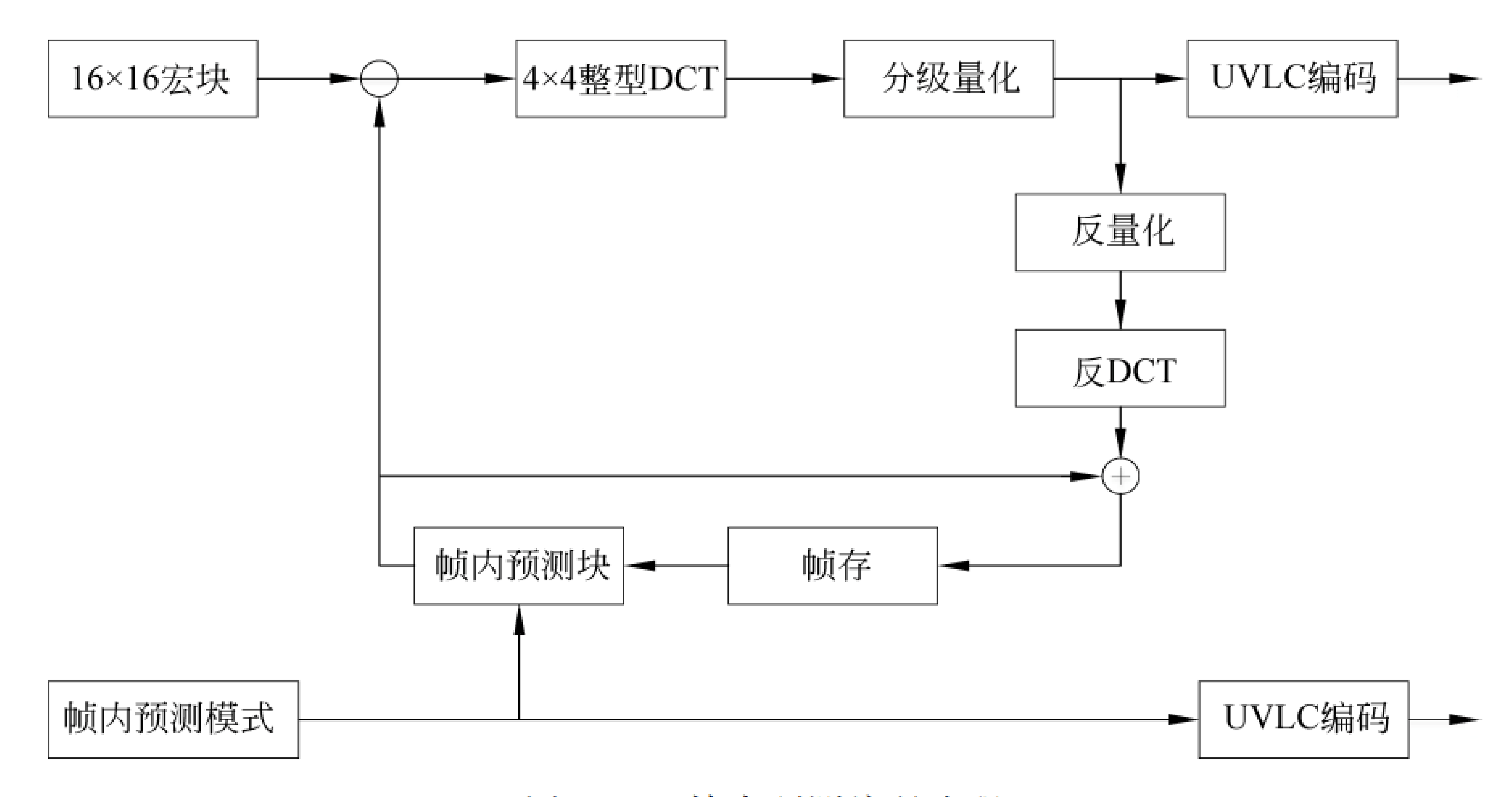


图 11-1 帧内预测编码流程

已编码重构的像素为参考像素进行预测。如图 11-2 所示，$A\sim M$ 是一个 4×4 块数据的参考像素，0～15 是 4×4 块的原始像素。在 H.264 中，帧内 4×4 亮度预测一共有 9 种预测模式。

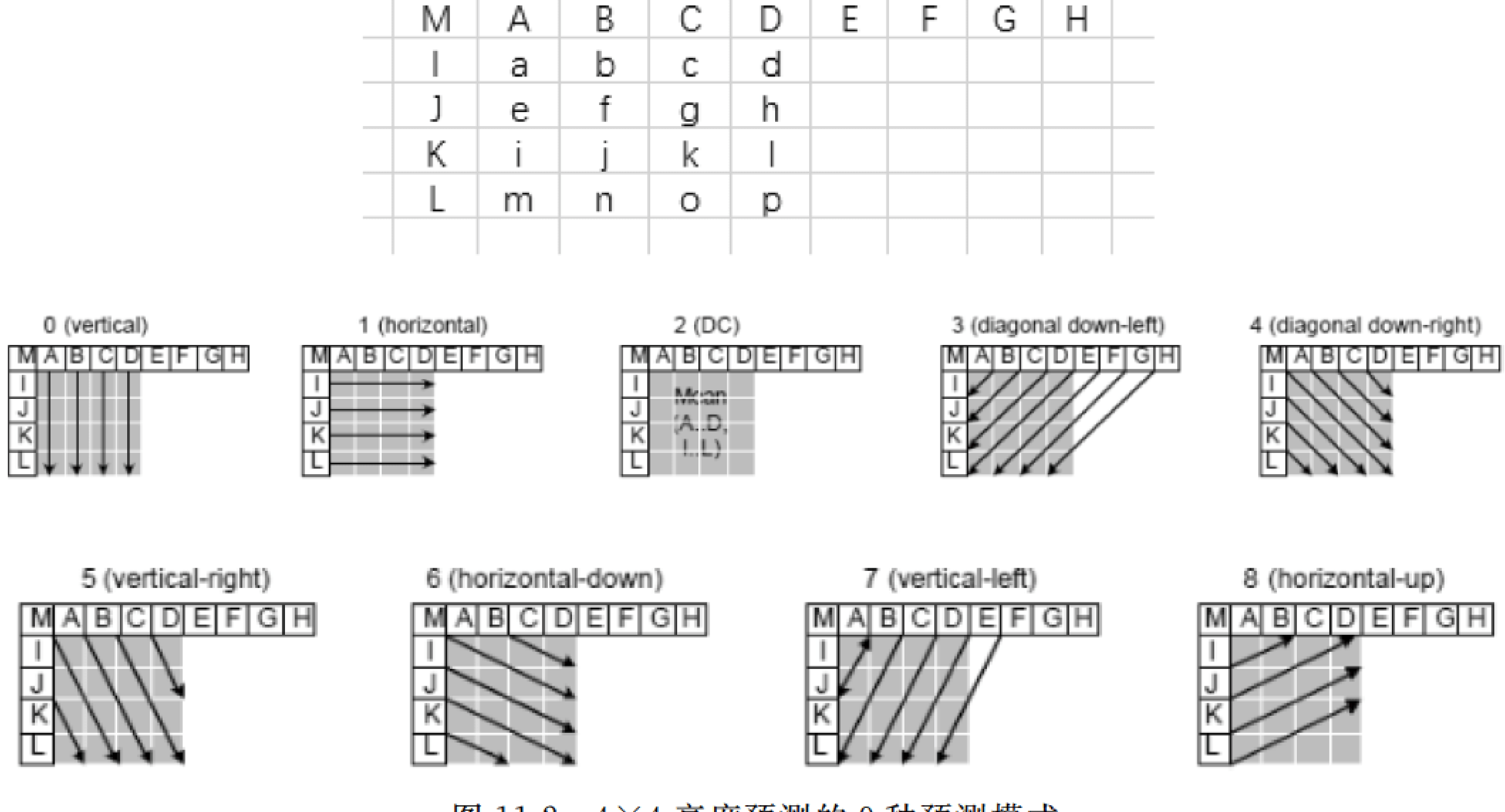


图 11-2 4×4 亮度预测的 9 种预测模式

(1) 模式 0(垂直模式)：当前宏块每列像素的预测值就是上边的参考像素。

当 A、B、C、D 4 个样本点都可用时，预测过程为

—a,e,i,m 由 A 预测

—b,f,j,n 由 B 预测

—c,g,k,o 由 C 预测

—d,h,l,p 由 D 预测

(2) 模式 1(水平模式):当前宏块每行像素的预测值就是左边的参考像素。

当 I、J、K、L 都可用时,预测过程为

—a,b,c,d 由 I 预测

—e,f,g,h 由 J 预测

—i,j,k,l 由 K 预测

—m,n,o,p 由 L 预测

(3) 模式 2(DC 模式):当前宏块所有像素的预测值就是上边和左边参考像素的平均值。

如果 A、B、C、D、I、J、K、L 都可用,则所有像素值为

$$(A+B+C+D+I+J+K+L+4)/8$$

如果 A、B、C、D 不可用,而 I、J、K、L 可用,则所有像素值为

$$(I+J+K+L+2)/4;$$

反之为$(A+B+C+D+2)/4$

如果 A、B、C、D、I、J、K、L 均不可用,则所有像素值为 128。

(4) 模式 3(下左对角线):由对应参考像素值加权得出相应像素的预测值。

当 A、B、C、D 都可用时,预测过程为

—a 预测为 $(A+2B+C+2)/4$;

—b、e 预测为 $(B+2C+D+2)/4$;

—c、f、i 预测为 $(C+2D+E+2)/4$;

—d、g、j、m 预测为 $(D+2E+F+2)/4$;

—h、k、n 预测为 $(E+2F+G+2)/4$;

—l、o 预测为 $(F+2G+H+2)/4$;

—p 预测为 $(G+3H+2)/4$;

(5) 模式 4(下右对角线):由对应参考像素值加权得出相应像素的预测值。

当 A、B、C、D、I、J、K、L 和 M 都可用时,预测过程为

—m 预测为$(J+2K+L+2)/4$;

—i,n 预测为$(I+2J+K+2)/4$;

—e,j,o 预测为$(M+2I+J+2)/4$;

—a,f,k,p 预测为$(A+2M+I+2)/4$;

—b,g,l 预测为$(M+2A+B+2)/4$;

—c,h 预测为$(A+2B+C+2)/4$;

—d 预测为$(B+2C+D+2)/4$。

(6) 模式 5(垂直向右):由对应参考像素值加权得出相应像素的预测值。

当 A、B、C、D、I、J、K、L 和 M 都可用时,预测过程为

—a,j 预测为$(M+A+1)/2$;

—b,k 预测为$(A+B+1)/2$;

—c,l 预测为$(B+C+1)/2$;

—d 预测为$(C+D+1)/2$;

—e,n 预测为(I+2M+A+2)/4;
—f,o 预测为(M+2A+B+2)/4;
—g,p 预测为(A+2B+C+2)/4;
—h 预测为(B+2C+D+2)/4;
—i 预测为(Q+2I+J+2)/4;
—m 预测为(I+2J+K+2)/4。
(7) 模式 6(水平向下):由对应参考像素值加权得出相应像素的预测值。
当 A、B、C、D、I、J、K、L 和 M 都可用时,预测过程为
—a,g 预测为(M+AI+1)/2;
—b,h 预测为(I+2M+A+2)/4;
—c 预测为(M+2A+B+2)/4;
—d 预测为(A+2B+C+2)/4;
—e,k 预测为(I+J+1)/2;
—f,l 预测为(M+2I+J+2)/4;
—i,o 预测为(J+K+1)/2;
—j,p 预测为(I+2J+K+2)/4;
—m 预测为(K+L+1)/2;
—n 预测为(J+2K+L+2)/4。
(8) 模式 7(垂直向左):由对应参考像素值加权得出相应像素的预测值。
当 A、B、C、D 都可用时,预测过程为
—a 预测为(A+B+1)/2;
—b,i 预测为(B+C+1)/2;
—c,j 预测为(C+D+1)/2;
—d,k 预测为(D+E+1)/2;
—l 预测为(E+F+1)/2;
—e 预测为(A+2B+C+2)/4;
—f,m 预测为(B+2C+D+2)/4;
—g,n 预测为(C+2D+E+2)/4;
—h,o 预测为(D+2E+F+2)/4;
—p 预测为(E+2F+G+2)/4。
(9) 模式 8(水平向上):由对应参考像素值加权得出相应像素的预测值。
当 I、J、K、L 都可用时,预测过程为
—a 预测为(I+J+1)/2;
—b 预测为(I+2J+K+2)/4;
—c,e 预测为(J+K+1)/2;
—d,f 预测为(J+2K+L+2)/4;
—g,i 预测为(K+L+1)/2;
—h,j 预测为(K+2L+M+2)/4;

—l,n,k,m,o,p 预测为 L。

11.2.2　帧内 16×16 亮度预测

当图像中细节信息较少时,就采用帧内 16×16 亮度预测模式。帧内 16×16 有 4 种预测模式,分别为垂直模式、水平模式、DC 模式、平面模式,如图 11-3 所示。

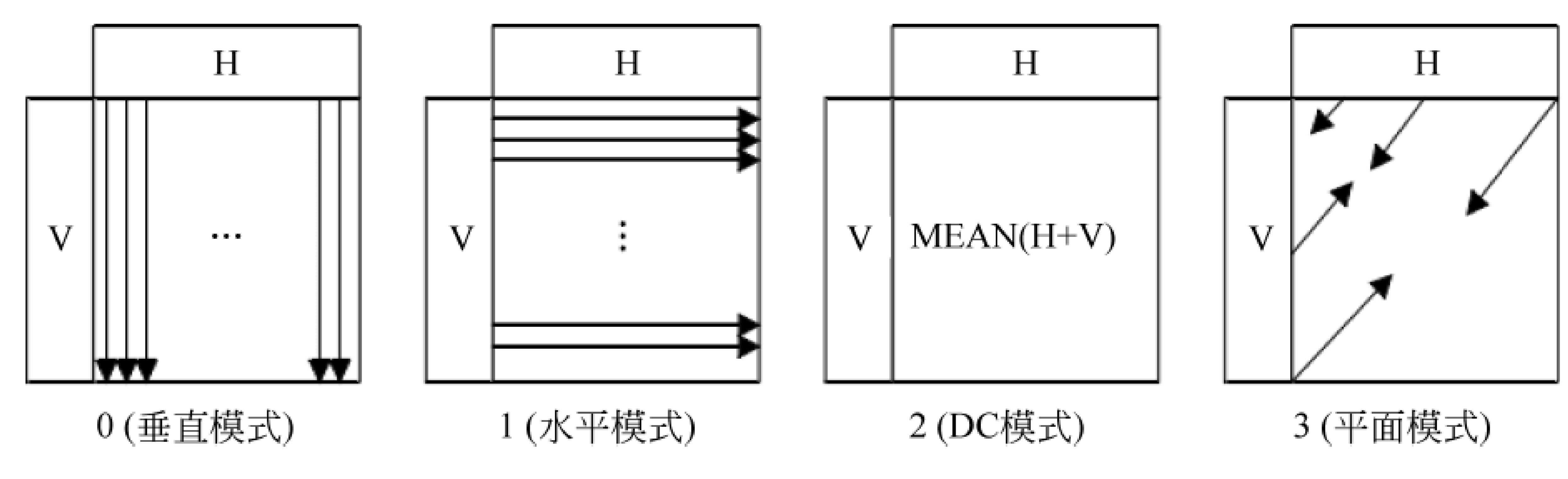


图 11-3　帧内 16×16 预测模式

为了便于分析,给图 11-3 中的参考像素和预测像素编上坐标。令 V 组元素从上到下的坐标依次为 $(-1, y)$, $y=0,1,2,\cdots,15$, H 组元素从左到右的坐标依次为 $(x,-1)$, $x=0,1,2,\cdots,15$ 。当前块左上角元素坐标为(0,0),往右为横坐标正方向,往下为纵坐标正方向;令 $p(x, y)$ 为坐标 (x, y) 点的像素值, $pred(x, y)$ 为块内坐标 (x, y) 点的预测值。下面以这个坐标系为基础,对 4 种模式进行分析。

(1) 模式 0:垂直预测。

该预测模式通过当前预测块正上方的 H 组元素进行预测,只有当 H 组元素进行预测,H 组元素都在图像内部时,此种预测模式才有效。块内各像素点的计算值如下。

$$pred(x, y) = p(x, -1), \quad x, y = 0,1,2,\cdots,15 \tag{11-1}$$

(2) 模式 1:水平预测。

该预测模式通过当前块正左侧的 V 组元素进行预测,只有当 V 组元素都在图像内部时,此种预测模式才有效。块内各像素点的计算值如下。

$$pred\ (x, y) = p(-1, y), \quad x, y = 0,1,2,\cdots,15 \tag{11-2}$$

(3) 模式 2:DC 预测。

该预测模式根据当前块 H 组元素和 V 组元素的有无,计算公式有所不同。当只有 V 组元素时,计算公式为

$$pred\ (x,y) = \left(\sum_{y=0}^{15} p(-1, y) + 8\right)/16, \quad x, y = 0,1,2,\cdots,15 \tag{11-3}$$

当只有 H 元素时,计算公式为

$$pred\ (x,y) = \left(\sum_{x=0}^{15} p(x, -1) + 8\right)/16, \quad x, y = 0,1,2,\cdots,15 \tag{11-4}$$

当 H 组和 V 组元素都存在时,计算公式为

$$pred\ (x,y) = \left(\sum_{x=0}^{15} p(x, -1) + \sum_{y=0}^{15} p(-1,y) + 16\right)/32, \quad x, y = 0,1,2,\cdots,15 \tag{11-5}$$

当 H 组和 V 组元素都不存在时，令当前块所有元素的预测值都为 128，计算公式为

$$pred(x,y) = 128, \quad x,y = 0,1,2,\cdots,15 \tag{11-6}$$

（4）模式 3：平面预测。

该预测模式通过当前预测块正上方的 H 组和正左侧的 V 组元素共同预测，因此只适合于 H 组元素和 V 组元素都存在的情况。对 H 组元素和 V 组元素，定义

$$H = \sum_{x=0}^{7}(x+1)(p(8+x,-1) - p(6-x,-1)) \tag{11-7}$$

$$V = \sum_{y=0}^{7}(y+1)(p(-1,8+y) - p(-1,6-y)) \tag{11-8}$$

$$a = 16 \times (\, p(-1,15) + p(15,-1)) \tag{11-9}$$

$$b = (5 \times H + 32) \,/\, 64 \tag{11-10}$$

$$c = (5 \times V + 32) \,/\, 64 \tag{11-11}$$

预测结果为

$$\begin{aligned} &pred(x,y) = clip((a + b(x-7) + c(y-7) + 16) \,/\, 32) \\ &x,y = 0,1,2,\cdots,15 \end{aligned} \tag{11-12}$$

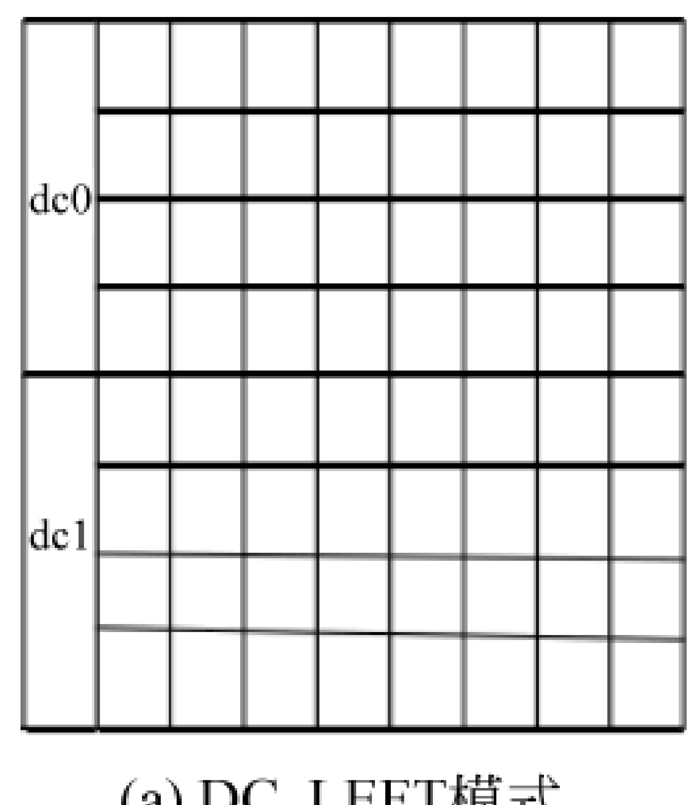
其中，$clip()$ 为限幅函数，定义为

$$clip(x) = \begin{cases} 0 & x < 0 \\ 255 & x > 255 \\ x & \text{其他} \end{cases} \tag{11-13}$$

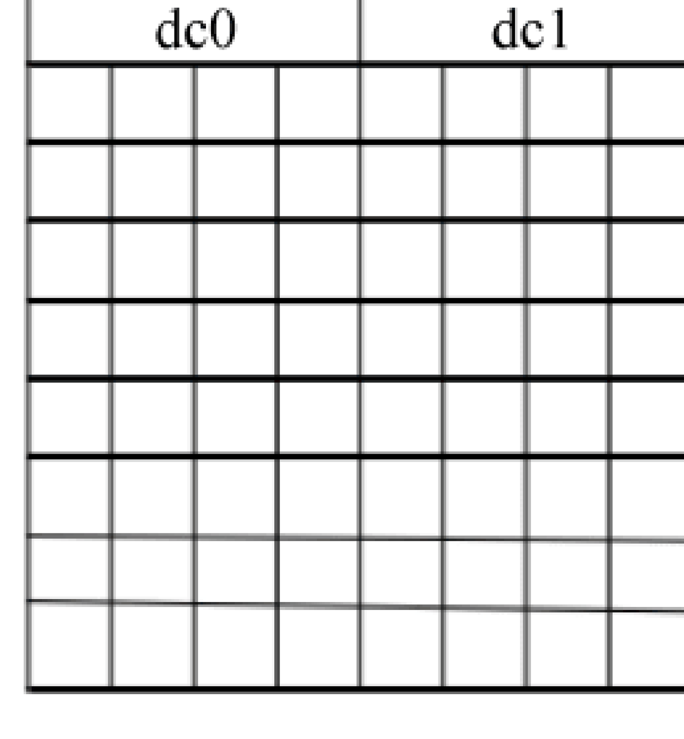
11.2.3 帧内色度 8×8 预测

要完成完整的视频显示，色度分量也是相当重要的一个因素。在采用 4∶2∶0 的 YUV 格式的视频源下，H.264 标准中将一个 16×16 亮度块和两个 8×8 的色度块合起来称为一个完整的宏块。因为相对来说，人眼对亮度的敏感性大于对色度的敏感性，所以色度的数据量较小，也完成了一个小量的压缩。

一个宏块中包含一个 8×8 块的色度 U 分量和一个 8×8 块的色度 V 分量，其预测方法和亮度 16×16 类似，也是 4 种模式：垂直模式、水平模式、DC 预测、平面预测，计算方法略有不同，如图 11-4 所示。



(a) DC_LEFT模式



(b) DC_TOP模式

S0 4×1　S1 4×1
S2 1×4　dc0 4×4　dc1 4×4
S3 1×4　dc2 4×4　dc3 4×4

(c) DC模式

图 11-4　帧内色度 8×8 DC 预测模式

(1) 垂直模式：当前宏块每列像素的预测值就是对应上边的参考像素。

(2) 水平模式：当前宏块每行像素的预测值就是对应左边的参考像素。

(3) DC 预测：根据宏块位置的不同，DC 又分为 4 种形式。

(a) DC_128：左边和上边都无参考像素时，预测值为 128。

(b) DC_LEFT：只有左边参考像素时，预测值如图 11-4(a)所示，上边 4×8 块像素的预测值为其对应左边 4 个参考像素的平均值，下边 4×8 块像素的预测值为其对应左边 4 个参考像素的平均值。

(c) DC_TOP：只有上边参考像素时，预测值如图 11-4(b)所示，左边 8×4 块像素的预测值为其对应上边 4 个参考像素的平均值。

(d) DC 模式：当左边和上边都有参考像素时，预测值如图 11-4(c)所示，dc0 等于其左边块 4 个像素 S2 和上边块 4 个像素 S0 的平均值；dc1 等于其上边块 4 个像素 S1 的平均值；dc2 等于其左边块 4 个像素 S3 的平均值；dc3 等于其左边块 4 个像素 S3 和上边块 4 个像素 S1 的平均值，这是以 dc 块的位置为基准进行上、下、左、右对应。

(4) 平面预测：该模式下的预测值算法如下。

$$pred(x, y) = Clip((a + b \times (x - 3) + c \times (y - 3) + 16)/32) \tag{11-14}$$

式(11-14)中，a、b、c 的值分别为

$$\begin{cases} a = 16 \times (p[-1,7] + p[7,-1]) \\ b = (17 \times H + 16)/32 \\ c = (17 \times V + 16)/32 \end{cases} \tag{11-15}$$

其中 H、V 分别为

$$\begin{cases} H = \sum_{x=0}^{3} (x+1) \times (pix[4+x,-1] - pix[2-x,-1]) \\ V = \sum_{y=0}^{3} (y+1) \times (pix[-1,4+y] - pix[-1,2-y]) \end{cases} \tag{11-16}$$

其中 $Clip()$ 函数是指括号内的数值如果大于 255，结果就是 255；如果小于 0，结果就是 0；如果为 0～255，就是其本身。

11.3 变换模块

H.264 标准中用到两种常见的矩阵运算：DCT[180] 和哈达玛变换[181]。

11.3.1 整数 DCT

H.264 标准采用整数 DCT 降低了以往标准中 DCT 操作浮点数的复杂性，避免了浮点数运算引入的舍入误差，只需通过加法和移位运算即可实现整个变换过程，从而保证了正逆变换操作数据的一致性。同时，结合 DCT 与后面的量化部分，使变换中的归一化运算与量化中的除法运算合并起来，并利用乘法与移位进行实现，从而消除浮点数 DCT 正变换与反变换不能完全匹配而产生的计算偏差。这样既简化了模块的复杂度，又保证了正逆变换数据的一致性，能够得到与标准 DCT 相似的编码效果。根据标准 4×4 DCT 的

定义,其变换公式如下。

$$\boldsymbol{Y}=\boldsymbol{AXA}^{\mathrm{T}} \tag{11-17}$$

这里,$\boldsymbol{A}$ 是单位正交矩阵,满足 $\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A}=\boldsymbol{I}$。

$$\boldsymbol{A}=\begin{bmatrix} \frac{1}{2}\cos(0) & \frac{1}{2}\cos(0) & \frac{1}{2}\cos(0) & \frac{1}{2}\cos(0) \\ \frac{1}{2}\cos\left(\frac{\pi}{8}\right) & \frac{1}{2}\cos\left(\frac{3\pi}{8}\right) & \frac{1}{2}\cos\left(\frac{5\pi}{8}\right) & \frac{1}{2}\cos\left(\frac{7\pi}{8}\right) \\ \frac{1}{2}\cos\left(\frac{2\pi}{8}\right) & \frac{1}{2}\cos\left(\frac{6\pi}{8}\right) & \frac{1}{2}\cos\left(\frac{10\pi}{8}\right) & \frac{1}{2}\cos\left(\frac{14\pi}{8}\right) \\ \frac{1}{2}\cos\left(\frac{3\pi}{8}\right) & \frac{1}{2}\cos\left(\frac{9\pi}{8}\right) & \frac{1}{2}\cos\left(\frac{15\pi}{8}\right) & \frac{1}{2}\cos\left(\frac{21\pi}{8}\right) \end{bmatrix} \tag{11-18}$$

设 $a=\frac{1}{2}, b=\sqrt{\frac{1}{2}}\cos\frac{\pi}{8}, c=\sqrt{\frac{1}{2}}\cos\frac{3\pi}{8}$,由余弦函数的周期性和对称性可得

$$\boldsymbol{A}=\begin{bmatrix} a & a & a & a \\ b & c & -c & -b \\ a & -a & -a & a \\ c & -b & b & -c \end{bmatrix}=\begin{bmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & a & 0 \\ 0 & 0 & 0 & b \end{bmatrix}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & d & -d & -b \\ 1 & -1 & -1 & 1 \\ d & -1 & 1 & -1 \end{bmatrix}=BC \tag{11-19}$$

其中 $d=c/b$,$\boldsymbol{B}$ 为对角矩阵。代入变换表达式,可得

$$\boldsymbol{Y}=\boldsymbol{BCXC}^{\mathrm{T}}\boldsymbol{B}=(\boldsymbol{CXC}^{\mathrm{T}})\cdot\boldsymbol{E}=(\boldsymbol{CXC}^{\mathrm{T}})\begin{bmatrix} a^2 & ab & a^2 & ab \\ ab & b^2 & ab & b^2 \\ a^2 & ab & a^2 & ab \\ ab & b^2 & ab & b^2 \end{bmatrix} \tag{11-20}$$

由于 a、b、c 都为实数,在计算机中需要考虑实数运算的复杂度和精确度问题,然而运算对象——像素值为整数,为了避免实数运算的复杂性,对 DCT 进行改进,将其改造成整数域中的运算。

对于矩阵 E 的运算,可以合并到后面的量化中,因此变换部分只需考虑 d(约等于 0.4142)的影响。为了进一步减少变换运算的复杂度,H.264 标准选定 $d=1/2$。同时,为了避免乘以 1/2 带来的截断误差,将 1/2 提到矩阵外,合并得到矩阵 E,这样得到修改后的公式为

$$\boldsymbol{Y}=(\boldsymbol{C}_f\boldsymbol{X}\boldsymbol{C}_f^{\mathrm{T}})\cdot\boldsymbol{E}_f$$

$$=\begin{bmatrix} 1 & 1 & 1 & 1 \\ 2 & 1 & -1 & -2 \\ 1 & -1 & -1 & 1 \\ 1 & -2 & 2 & -1 \end{bmatrix}\boldsymbol{X}\begin{bmatrix} 1 & 2 & 1 & 1 \\ 1 & 1 & -1 & -2 \\ 1 & -1 & -1 & 2 \\ 1 & -2 & 1 & -1 \end{bmatrix}\cdot\begin{bmatrix} a^2 & ab/2 & a^2 & ab/2 \\ ab/2 & b^2/4 & ab/2 & b^2/4 \\ a^2 & ab/2 & a^2 & ab/2 \\ ab/2 & b^2/4 & ab/2 & b^2/4 \end{bmatrix} \tag{11-21}$$

为了保证正逆变换的一致性,矩阵 $\boldsymbol{A}$ 需要满足正交性,即满足 $\boldsymbol{AA}^{\mathrm{T}}=\boldsymbol{I}$,因此可以定义 $a=1/2$,求得 $b=\sqrt{2/5}$。

这样就得到了 H.264 的整数 DCT 公式,其整个计算过程都在整数域中进行,变换核

$S=C_f X C_f^{\mathrm{T}}$ 只通过加减法或左移操作即可实现，后面的点乘运算也可以方便地合并到量化过程中。

同样，可以推出 IDCT 整数变换公式为

$$X= C_i^{\mathrm{T}}(Y \cdot E_i)C_i$$

$$=\begin{bmatrix}1 & 1 & 1 & 1/2\\ 1 & 1/2 & -1 & -1\\ 1 & -1/2 & -1 & 1\\ 1 & -1 & 1 & -1/2\end{bmatrix}\left[Y\cdot\begin{bmatrix}a^2 & ab & a^2 & ab\\ ab & b^2 & ab & b^2\\ a^2 & ab & a^2 & ab\\ ab & b^2 & ab & b^2\end{bmatrix}\right]\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & 1/2 & -1/2 & -1\\ 1 & -1 & -1 & 1\\ 1/2 & -1 & 1 & -1/2\end{bmatrix}$$

(11-22)

注意，不同于正向变换，反向变换并没有将 1/2 从变换矩阵中提取出来，这样虽然会产生截断误差，但可以获得更大的输出动态范围。

11.3.2　哈达玛变换

H.264 标准中对经过 DCT 的 DC 系数再次进行哈达玛变换。H.264 标准中的变换过程如图 11-5 所示。

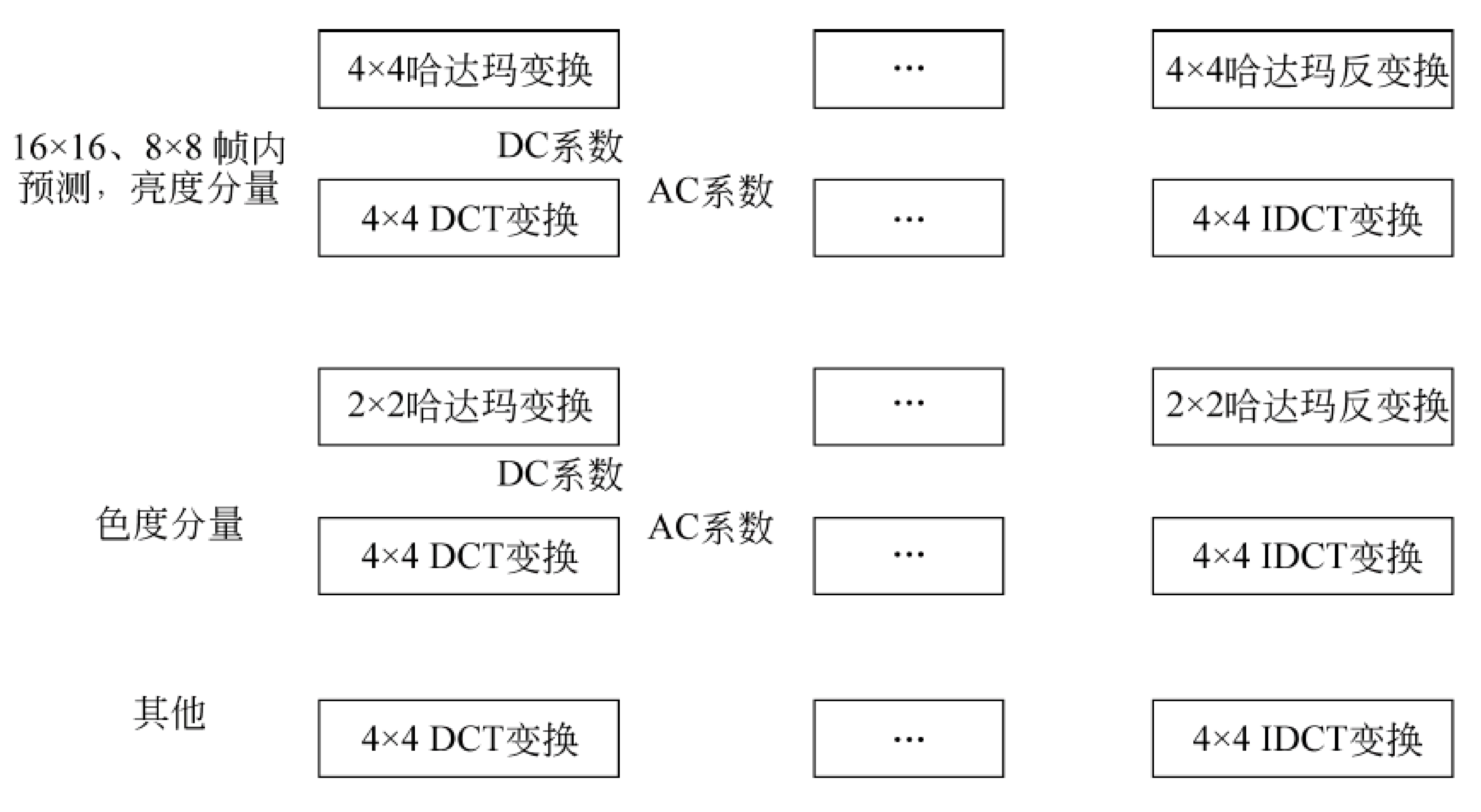


图 11-5　H.264 标准中的变换过程

H.264 将亮度分量的每个 16 阶宏块分解为 16 个 4 阶二维矩阵进行 DCT，然后将变换结果中的 DC 系数提取出来，组成一个 4 阶的亮度 DC 块，再对其进行 Hadamard 变换。同样，对于色度分量，将其子矩阵经过 DCT 后的 DC 系数提取出来，组成一个 2 阶的亮度 DC 块，再对其进行 Hadamard 变换。

H.264 标准中 4×4 哈达玛正、逆变换公式如下。

$$Y^{D4}=\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\\ 1 & -1 & 1 & -1\end{bmatrix}X^{D4}\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\\ 1 & -1 & 1 & -1\end{bmatrix}/4 \qquad (11\text{-}23)$$

$$X^{D4} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{bmatrix} Y^{D4} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{bmatrix} /4 \tag{11-24}$$

2×2 哈达玛正、逆变换公式如下。

$$Y^{D2} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} X^{D2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} /2 \tag{11-25}$$

$$X^{D2} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} Y^{D2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} /2 \tag{11-26}$$

与 DCT 相比，哈达玛变换没有缩放因子 E_f 或 E_i 的点乘运算，无须与后面的量化部分合并。哈达玛变换的系数均为±1，只用简单的加法运算即可实现。

11.4 量化模块

H.264 标准[181]中使用的是标量量化器，满足下列条件。

(1) 采用加法、减法、移位等算术运算，避免除法等浮点运算。

(2) 融合正向变换矩阵 E_f 和反向变换矩阵 E_i 的缩放因子运算。

量化的基本公式为：$Z_{ij} = round(Y_{ij}/Qstep)$，$Y_{ij}$ 为经过变换的残差值，$Qstep$ 为量化步长。

H.264 标准采用分级量化提高码率控制能力，提供了 52 个级别的量化参数(Quantization Parameter，QP)。QP 的取值范围为 0～51(亮度 QP 的最大值为 51，色度 QP 的最大值为 39)，每个 QP 值对应一个量化步长 $Qstep$，QP 值每增加 1，量化步长增加 12.25%，QP 每增加 6，$Qstep$ 增加 1 倍。随着 QP 值的增大，量化的精细度逐步降低。这样，周期性变化量化步长的好处是可以显著减少量化表和反量化表的大小，见表 11-1。

表 11-1　H.264 中量化步长 *Qstep* 与量化参数 QP 索引对照表

QP	*Qstep*	QP	*Qstep*	QP	*Qstep*	QP	*Qstep*
0	0.625	9	1.75	18	5	27	14
1	0.6875	10	2	19	5.5	28	16
2	0.8125	11	2.25	20	6.5	29	18
3	0.875	12	2.5	21	7	30	20
4	1	13	2.75	22	8	31	22
5	1.125	14	3.25	23	9	32	26
6	1.25	15	3.5	24	10	33	28
7	1.375	16	4	25	11	34	32
8	1.625	17	4.5	26	13	35	36

续表

QP	Qstep	QP	Qstep	QP	Qstep	QP	Qstep
36	40	40	64	44	104	48	160
37	44	41	72	45	112	49	176
38	52	42	80	46	128	50	208
39	56	43	88	47	144	51	224

矩阵 $\boldsymbol{E}_f$中的缩放因子 a^2、$ab/2$、$b^2/4$ 被整合到正向量化器中，直接对变换核 $\boldsymbol{S}=\boldsymbol{C}_f\boldsymbol{X}\boldsymbol{C}_f^{\mathrm{T}}$量化，量化后的系数变为

$$Z_{ij}=round\left(S_{ij}\frac{PF}{Qstep}\right) \tag{11-27}$$

其中，PF 是矩阵 $\boldsymbol{E}_f$中的缩放因子，为了避免除法操作，$PF/Qstep$ 可以用乘法因子 MF 和右移实现，即令

$$MF=\frac{PF}{Qstep}2^{qbits},\quad qbits=15+floor(QP/6) \tag{11-28}$$

H.264 标准中规定了乘法因子的取值，见表 11-2。

表 11-2　乘法因子 *MF* 的取值

QP	样点位置		其他位置	QP	样点位置		其他位置
	(0,0),(2,0),(0,2),(2,2)	(1,1),(1,3),(3,1),(3,3)			(0,0),(2,0),(0,2),(2,2)	(1,1),(1,3),(3,1),(3,3)	
0	13117	5243	8066	3	9362	3647	5825
1	11916	4660	7490	4	8192	3355	5243
2	11082	4194	6554	5	7282	2893	4559

这样就可以得到 H.264 中具体的量化过程表达式：

$$Z_{ij}=(S_{ij}\cdot MF_{ij}+f)>>qbits \tag{11-29}$$

f 为偏移量，其作用是改善恢复图像的视觉效果。帧内预测时，$f=2^{qbits}/3$；帧间预测时，$f=2^{qbits}/6$。

同样，可以推出反量化过程的表达式为

$$Y'_{ij}=(Z_{ij}\cdot V_{ij})<<floor(\mathrm{QP}/6) \tag{11-30}$$

乘法因子 V 的取值见表 11-3。

表 11-3　乘法因子 *V* 的取值

QP	位　置			QP	位　置		
	(0,0),(0,2),(2,0),(2,2)	(1,1),(1,3),(3,1),(3,3)	其他位置		(0,0),(0,2),(2,0),(2,2)	(1,1),(1,3),(3,1),(3,3)	其他位置
0	10	16	13	3	14	23	18
1	11	18	14	4	16	25	20
2	13	20	16	5	18	29	23

为了更好地支持对高清视频的编码，H.264标准引入了非一致性量化，即不同位置上的变换系数的量化步长不一样。通过对量化步长的调整，可以使编码的图像更适合人类视觉系统，更真实。同时也提供了一种控制编码质量的方式。

H.264使用量化权重矩阵 **W** 记录不同位置上的权重系数。量化权重越大，量化步长越短，量化结果越精细。为了在计算机中表示，**W** 中的系数是权重的16倍。标准中预定义了两个默认的量化权重系数矩阵 $Flat_4\times4_16$ 和 $Flat_8\times8_16$，在编码器没有使用自定义的量化权重矩阵时，解码器会使用这两个默认的权重矩阵。

$$W_{ij}\begin{cases}Flat_4\times4_16[i][j]=16, & i,j=0,1,2,3\\ Flat_8\times8_16[i][j]=16, & i,j=0,1,\cdots,7\end{cases} \tag{11-31}$$

这时，反量化公式化为

$$Y'_{ij}=\begin{cases}(Z_{ij}\cdot W_{ij}\cdot V_{ij}+2^{3-QP/6})>>4-\mathrm{QP}/6, \mathrm{QP}<24\\ (Z_{ij}\cdot W_{ij}\cdot V_{ij})<<\mathrm{QP}/6-4, \mathrm{QP}\geqslant 24\end{cases} \tag{11-32}$$

式中，Y_{ij} 是矩阵 **Y** 中的转换系数；Z_{ij} 是输出的量化系数；$Q\,step$ 是量化步长。H.264量化过程还要同时完成DCT中Ef乘法运算，它可以表述为

$$Z_{ij}=round(W_{ij}PF/Q\,step) \tag{11-33}$$

式中，W_{ij} 是矩阵 **W** 中的转换系数；PF 是矩阵 ***EF*** 中的元素。根据样本点在图像中的位置(i,j)取值，见表11-4。

表 11-4　*PF* 的取值

位置1	位置2	其他位置
(0,0),(2,0),(0,2),(2,2)	(1,1),(1,3),(3,1),(3,3)	其他情况
a^2	$b^2/4$	$ab/2$

利用量化步长随量化参数每增加6而增加1倍的性质，可以进行一步简化计算，即

$$\begin{aligned}qbits&=15+floor\ (\mathrm{QP}/6)\\ MF&=(PF/Qstep)2^{qbits}\end{aligned} \tag{11-34}$$

式中，$floor()$为取整函数（其输出不大于输入实数的最大整数），所以可将式(11-34)写为

$$Z_{ij}=round(W_{ij}\,MF/2^{qbits} \tag{11-35}$$

11.5　熵编码模块

H.264标准[181]采用基于上下文的自适应编码算法对语法元素进行编码。在基本档次采用上下文自适应的可变长编码(Context Adaptive Variable Length Coding, CACLC)；在主档次采用上下文自适应的二进制算术编码(Context Adaptive Binary Arithmetic Coding, CABAC)。

CAVLC用于对亮度和色度的残差数据进行熵编码。编码宏块的残差经变换、量化和Zigzag扫描后，具有以下特性。

(1) 残差块经变换、量化后，其非零系数主要集中在低频部分，高频部分的系数大部

分为零。

(2) 低频位置的非零系数的数值比较大,而高频部分上的非零系数的数值多为+1和−1。

(3) 非零系数的幅值变化有一定的规律和相关性,非零系数的游程也有一定的特性。

(4) 相邻的 4×4 块的非零系数的个数具有一定的关联性。

CAVLC 有效利用相邻编码符号的关联特性为当前编码符号选择合适的上下文模型,降低了符号编码间的信息冗余度。在 CAVLC 中,上下文模型的选择主要体现在:对各类非零量化系数的大小、位置给以独立的编码;自适应更新编码非零系数所需码表与系数后缀长度。

11.6　基于 H.264 的网络视频隐密通信

随着 H.264 视频压缩标准的提出和推广,基于 H.264 的信息隐藏算法层出不穷,但现有众多的算法仅考虑视频压缩编码得到的运动矢量或只注重视频图像的复杂度,而忽略了将二者相结合的方法。根据 H.263/4 等视频编/解码标准,帧间压缩运动矢量越大,表示视频内容变化越剧烈,相关的目标图像块运动变化越大,对这些区域适当改动所引起的失真易被人眼忽视。从信息隐藏的角度,运动矢量大相对于运动矢量小或者无运动的目标区域适合分布更多的密信。与此同时,帧内压缩编码则更期望保留纹理复杂区域和目标区域,而对于简单的背景以及平坦区域则采取大的压缩。从信息隐藏的角度,应该将密信隐藏在图像中纹理/边缘复杂的区域,避免密信出现在平坦区域。因为内容复杂也就意味着相应的区域能够给密信提供更安全的掩蔽空间,也能增加密信的嵌入容量,在有噪声干扰的信道下传输,能够使得密信的误码率降低,从而提高隐密传输的可靠性。

11.6.1　视频内容复杂度分析

为筛选出纹理复杂、运动剧烈、掩蔽性高的区域,视频内容复杂度分析包含视频图像纹理估计和视频帧间运动估计两个方面。

1) 视频图像纹理估计

基于模糊熵[12]的帧图像纹理复杂度估计已经在之前的章节里做了详细论证,这里不再赘述。结合本章以下内容,这里只给出一个 $m\times n$ 大小的图像块的平均模糊熵测度的定义。

$$R_{B_i} = \frac{1}{m\times n}\sum_{x}^{m}\sum_{y}^{n}R(x,y) \tag{11-36}$$

其中,B_i 表示第 i 个 $m\times n$ 大小的亮度图像块,称它为当前块;R_{B_i} 表示其纹理复杂度;$R(x,y)$表示坐标为(x,y)处的模糊熵测度。

2) 视频帧间运动估计

根据 H.264 视频压缩标准对视频进行帧间运动估计[179],得到一个 $m\times n$ 大小的图像块的运动矢量为$(\boldsymbol{H}_{B_i},\boldsymbol{V}_{B_i})$,通过欧氏距离求其运动矢量的大小:

$$S_{B_i} = \sqrt{\boldsymbol{H}_{B_i}^2+\boldsymbol{V}_{B_i}^2} \tag{11-37}$$

其中，S_{B_i}为当前块运动矢量的大小；$\boldsymbol{H}_{B_i}$、$\boldsymbol{V}_{B_i}$分别为当前块相对于预测块在水平和垂直方向上的偏移量。

3）视频复杂度的定义

定义 11.1 结合视频帧图像的纹理和运动估计，预嵌密视频内容复杂度为

$$F_{B_i} = R_{B_i} \times \rho + S_{B_i} \times (1-\rho) \tag{11-38}$$

其中，ρ为均衡系数（$0 \leqslant \rho \leqslant 1$），$F_{B_i}$为当前块的复杂度。

11.6.2 隐密信道构建

1. 隐密信道的定义

定义 11.2 待嵌密候选载体集合为$\{C_l\}_{l=1}^{\infty}=\{B_1, B_2, \cdots, B_l\}$，$B_l \in I, F_{B_i} \geqslant TH$，其中$I$为视频参考帧，$l$为集合中载体的数量，$TH$为复杂度阈值。

定义 11.3 隐密信道定义为：$\{C_{k_i}\}=\{B_1, B_2, \cdots, B_{|M|}\} \in \{C_l\}_{l=1}^{\infty}$，其中$|M|$为密信空间大小。在密钥空间$K$中，$\forall k_i, k_j \in K: k_i \neq k_j \rightarrow \{C_{k_i}\} \neq \{C_{k_j}\}$，$k_i$、$k_j$分别表示密钥空间中的一个随机抽样。

2. 载体嵌入容量

隐密信道中各载体块的嵌入容量D_{B_i}为

$$D_{B_i} = ceil(F_{B_i} \times X) \tag{11-39}$$

其中，$ceil(\cdot)$表示向上取整函数，X为载体图像块可嵌入的最大密信容量。

3. 密钥共享与变换

隐密变换过程如算法 11.1 所示。

算法 11.1

① 接收方预先将自己的临时口令k_1传输给发送方，发送方将自己的临时口令k_2与k_1进行杂凑，得到密钥对(n_1, k_1)和(n_2, k_2)。

② 发送方根据密钥(n_1, k_1)将密信进行置乱$\Gamma_{M'}=A_N^{(n_1,k_1)} \times \Gamma_M$，根据密钥对$(n_2, k_2)$置乱载体嵌入顺序$\Gamma_{C'}=A_N^{(n_1,k_1)} \times \Gamma_C$。

③ 按照 8.5.3 节的过程将密信嵌入在视频流中，并将自己的临时口令k_2通过其他通道传输给接收方。

④ 接收方根据k_1和k_2采用同样的杂凑算法求出密钥对(n_1, k_1)和(n_2, k_2)。

⑤ 根据密钥对(n_2, k_2)将载体提取顺序进行逆变换$\Gamma_C=(A_N^{(n_2,k_2)})^{-1} \times \Gamma_{C'}$，并提取出密信；再根据$(n_2, k_2)$将提取出的密信进行逆变换，得到原始秘密信息$\Gamma_M=(A_N^{(n_1,k_1)})^{-1} \times \Gamma_{M'}$。

其中，Γ_M表示原始秘密信息分布，$\Gamma_{M'}$为其置乱后的分布；Γ_C表示原始载体嵌入顺序，$\Gamma_{C'}$为其置乱后的嵌入顺序；$A_N^{(n_i,k_i)}$代表 Arnold 变换矩阵，n_1, k_1与n_2, k_2为变换参数；N为置乱空间。

密钥杂凑算法如算法 11.2 所示。

算法 11.2

① 拼接口令k_1与k_2，采用 MD5 对其加密，得到口令比特流。

② 将口令比特流首尾对折进行异或操作，直到口令比特变为 32 位。

③ 将 32 位的口令比特流分为 4 部分，转化为十进制，分别得到密钥对 n_1, k_1 和 n_2, k_2 的值。

采用上述密钥共享算法能够有效防止模仿攻击。对于接收方和发送来说，每次通信均采用临时口令进行杂凑，即使知道自己的临时口令，也无法由此推测出密钥对的值；而对于第三方攻击的情况，如果攻击者想从含密视频流中正确提取出密信，就必须同时知道收发双方的临时口令，或者知道密钥对的各参数值，要满足这两种方式成立的条件均十分困难。

11.6.3　密信嵌入与提取

设一个 $m\times n$ 大小的载体块的亮度矩阵表示为 $\boldsymbol{B}_{m\times n}$，这里我们称其为当前块，经过帧内预测估计后得到的预测块记为 $\boldsymbol{R}_{m\times n}$。编码时，编码器将当前块与预测块求差，得到的残差矩阵 $\boldsymbol{D}_{m\times n}$ 可表示为

$$D_{m\times n} = B_{m\times n} - R_{m\times n} = d(i,j)_{m\times n},\quad 0 \leqslant i < m; 0 \leqslant j < n \tag{11-40}$$

在视频压缩过程中，编码器将对残差矩阵进行 DCT、量化操作。本章采用 LSB 算法，若当前块属于隐密信道，则将预处理后的密信嵌入在其量化残差块的中频系数中，得到含密量化残差块 $\boldsymbol{D}'_{m\times n}$，否则进行一般的帧内预测过程。然后再进行逆量化、逆 DCT 处理为含密残差矩阵 $\hat{\boldsymbol{D}}'_{m\times n}$，该过程可表示为

$$\hat{\boldsymbol{D}}'_{m\times n} = iDCT(iQ(\boldsymbol{D}'_{m\times n})), \boldsymbol{D}'_{m\times n} = LSB(DCT(Q(\boldsymbol{D}_{m\times n})), m_i) \tag{11-41}$$

其中，$DCT(\cdot)$为 DCT ，$iDCT(\cdot)$为逆 DCT，$Q(\cdot)$代表量化操作，$iQ(\cdot)$为逆量化操作，$LSB(\cdot)$为 LSB 嵌入操作。根据 $\boldsymbol{D}'_{m\times n}$ 和 $\boldsymbol{R}_{m\times n}$ 得到含密重构块 $\widehat{B}'_{m\times n}$：

$$B'_{m\times n} = R_{m\times n} + D'_{m\times n} \tag{11-42}$$

再将 $\widehat{B}'_{m\times n}$ 作为下一当前块的参考像素块，继续进行帧内预测，直到密信嵌入完毕，则继续按照 H.264 压缩标准对后续视频序列进行处理。

接收方收到含密视频序列后进行解码得到含密量化残差块 $\boldsymbol{D}'_{m\times n}$，根据密钥 n_2, k_2 在相应的中频系数中提取秘密信息，再根据密钥 n_1, k_1 对密信进行逆 Arnold 变换，得到原始秘密信息。

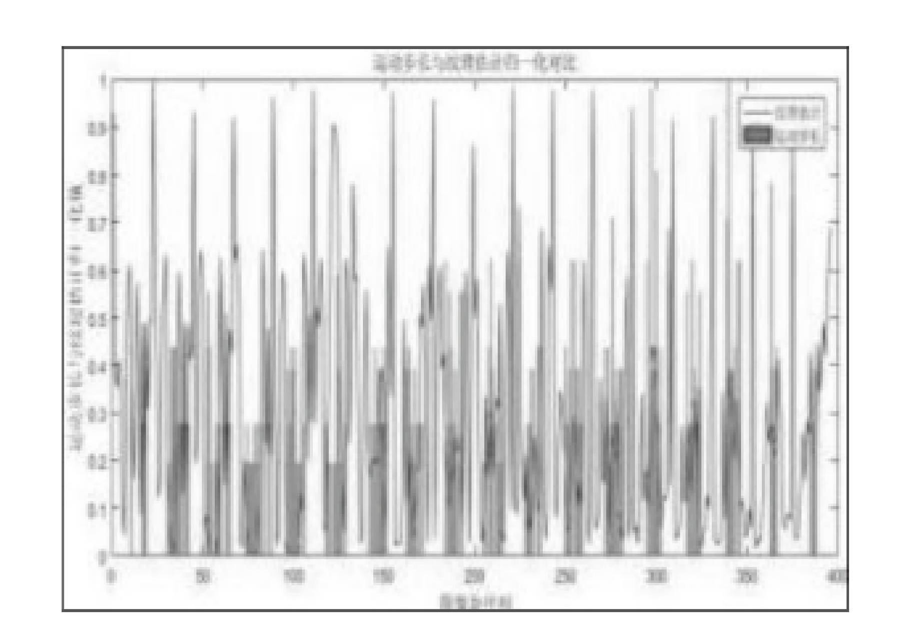
11.6.4　实验结果

使用 8 段典型的 YUV 标准视频序列（176×144，150 帧）进行分析，以误码率、失真率、码长改变率作为参考指标，选择最新的基于 DCT 系数的视频隐密算法[182]（对比算法 1）和基于运动矢量的密信嵌入算法[183]（对比算法 2）作为对比算法，如图 11-6 所示。

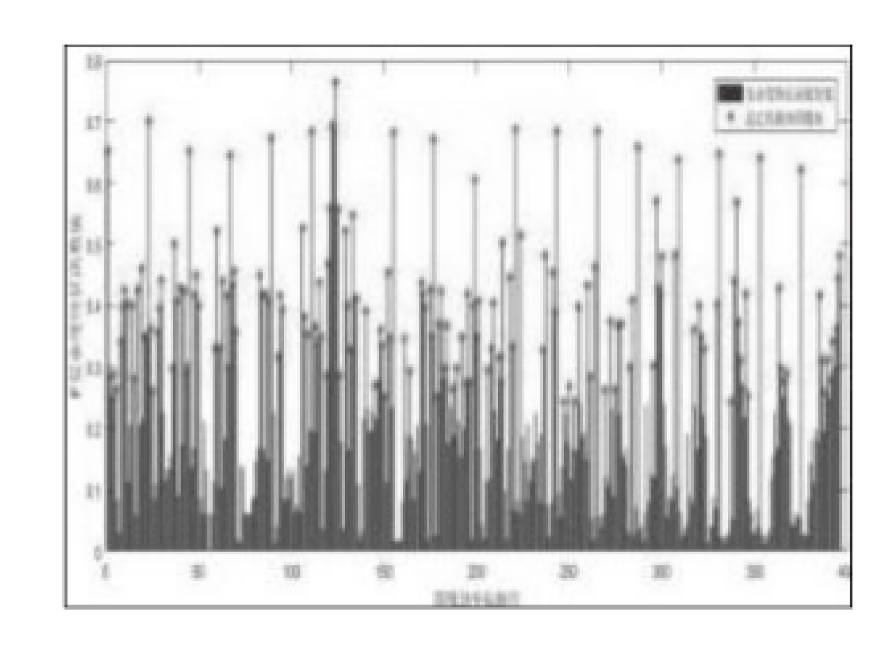
1. 算法自适应性能测试

图 11-6(a)为参考帧内容分析，两类线段分别为纹理复杂度与运动步长归一化值；图 11-6(b)为参考帧图像块复杂度估计，′ * ′表示候选载体集合；图 11-6(c)是根据临时密钥随机抽取的一组隐密信道样本，理想情况下为一密一信道；图 11-6(d)为隐密信道嵌入权值的相对变化情况，权值不同，嵌入量不同。从效果看，所选载体块的位置分布在纹理

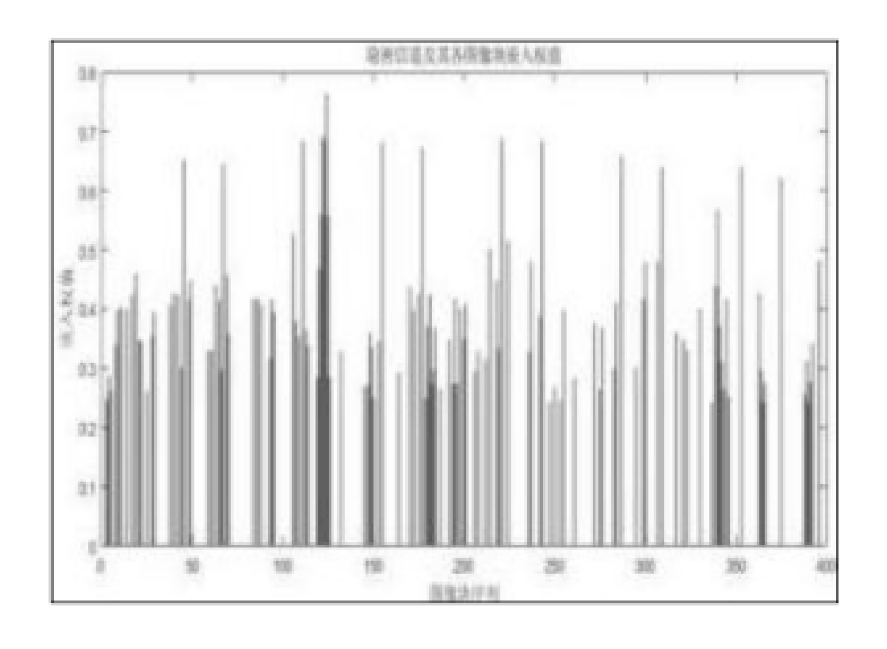
复杂且运动剧烈的区域,并且嵌入权值的变化与视频图像内容的变化一致。



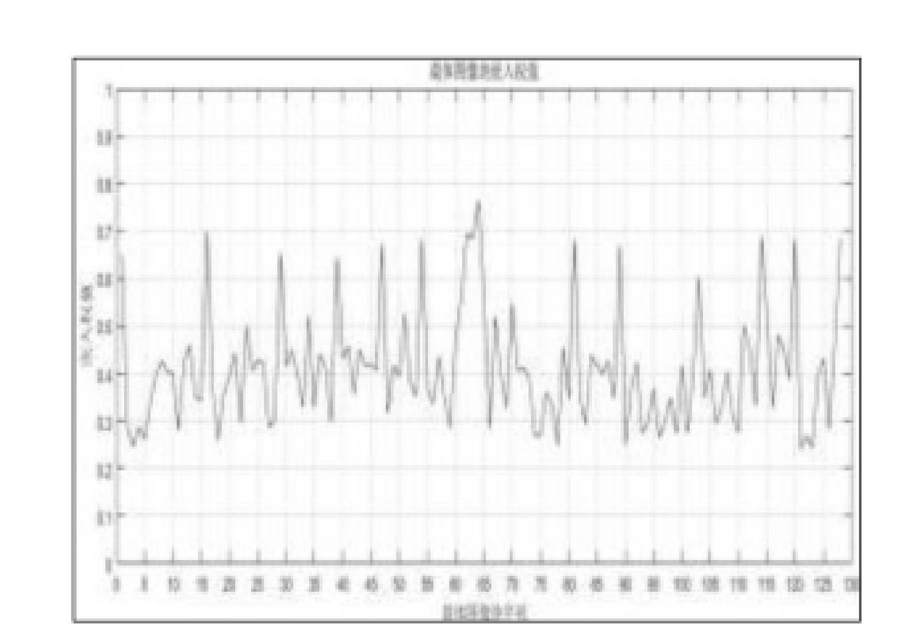
(a) 纹理和运动变化情况



(b) 候选载体及复杂度估计



(c) 隐密信道抽样样本



(d) 嵌入权值相对变化情况

图 11-6　隐密信道构建过程及其嵌入权值

2. 误码率对比测试

为了对比基于 DCT 系数的视频隐密算法[182]、基于运动矢量的密信嵌入算法[183]以及自适应视频内容的信息隐藏算法在不同视频序列中的误码率大小,分别选择 FOREMAN 等 8 段视频序列进行算法仿真,结果见表 11-5。

表 11-5　各算法在不同视频序列中的误码率对比,其中黑体表示最优性能

(单位:bit)

视频序列	对比算法 1	对比算法 2	本章算法
FOREMAN	0.5599	0.2545	**0.0178**
BUS	0.5476	0.2308	**0.0119**
CITY	0.4583	0.1705	**0.0060**
FOOTBALL	0.5060	0.2091	**0.0774**
HARBOUR	0.4940	0.3000	**0.0595**
ICE	0.5000	0.2432	**0.0119**
MOBILE	0.4524	0.2091	**0.0595**
SOCCER	0.4405	0.1955	**0.0179**

由表 11-5 可知,本章算法将密信嵌入在图像块 DCT 量化后的系数中,密信提取依然保持着低的误码率。

3. 失真率对比结果

由于各类算法的效果均是人眼不可感知的，为精确量化失真程度，引入峰值信噪比(Peak Signal to Noise Ratio，PSNR)进行失真率对比，结果见表 11-6。

表 11-6　各算法在不同视频序列中的 PSNR 对比，其中黑体表示最优性能

(单位：dB)

视频序列	对比算法 1	对比算法 2	本章算法
FOREMAN	35.5784	35.5762	**35.5958**
BUS	**33.0665**	32.2857	33.0477
CITY	33.9261	33.0850	**33.9451**
FOOTBALL	32.6296	**32.6442**	32.5955
HARBOUR	33.1227	32.9581	**33.1631**
ICE	36.1373	35.7249	**36.1631**
MOBILE	**31.5405**	31.0613	31.5186
SOCCER	34.5683	33.5594	**34.5819**

从表 11-6 中可以看出，本章算法将密信嵌入在掩蔽性高的图像块中，PSNR 值较优于对比算法。

4. 码长改变率与误码率对比结果

为了精确评估在相同压缩强度下(选择编码器默认固定量化步长，quant＝4)本算法与对比文献算法对视频码长的改变情况，引入码长改变率

$$CLR = (OL - EL) / OL \tag{11-43}$$

其中，CLR 为码长改变率，OL 为原始视频码长，EL 为含密视频码长，对比结果见表 11-7。

表 11-7　各算法在不同视频序列中的码长改变率对比，其中黑体表示最优性能

视频序列	对比算法 1	对比算法 2	本章算法
FOREMAN	**0**	0.0179	6.1974e-04
BUS	8.2077e-04	0.0301	**2.4623e-04**
CITY	7.5031e-04	0.0311	**2.5792e-04**
FOOTBALL	2.5599e-04	0.0279	**1.5753e-04**
HARBOUR	**2.3461e-04**	0.0303	5.4742e-04
ICE	4.4303e-04	0.0134	**1.7229e-04**
MOBILE	8.5425e-04	0.0320	**2.2999e-04**
SOCCER	**2.9230e-04**	0.2798	4.3846e-04

从表 11-7 中可以看出，对比算法 1 将密信平铺嵌入在 DCT 系数中，对原始视频改变小，码长变化较小；对比算法 2 之所以改变较大，是因为其用非最优匹配块的差值替换了最优匹配块的差值，导致量化压缩后非零系数增大，码长改变明显。本章算法将密信嵌入在复杂度高的区域中，做到了尽量避免修改零值 DCT 量化系数，因而视频码长改变较小。

第 12 章 基于移动终端的隐密系统开发

手机用户频繁使用各类应用软件,使得大量个人私密数据存留在手机和网络中。这些敏感数据面临着泄露、窃取等多方面的潜在威胁,特别是在网络应用背景下更是缺乏对敏感数据传输及存储的安全保护。

本章讨论信息隐藏技术在实时通信系统中的应用,介绍了基于 Android 系统的移动终端实时隐密的设计以及实现。

12.1 网络即时通信技术

12.1.1 即时通信技术

网络即时通信应用将文字、图像、音视频、文件等多媒体通信业务集成于一体,其最基本的特征就是信息传递的实时性和用户交互的便捷性。与传统通信模式相比,即时通信技术具有通信成本低、效率高、实时性强等优点。

即时通信软件涉及的网络协议主要包括 IP、TCP、UDP、RMTP 等。根据应用背景的不同,即时通信技术可采用 C/S 通信模式、P2P 模式以及基于 C/S 和 P2P 的混合模式。

12.1.2 即时通信系统中的安全性诉求

即时通信系统面临的安全威胁主要来自以下 3 个方面。

(1) 用户主要面临的威胁是针对客户端的攻击,主要包括信息窃听、泄露:目前的系统中一般只对密码进行加密处理,而通信内容几乎都是明文传输,利用简单的网络嗅探器就可以轻易还原消息内容,极易被第三方窃听,造成信息泄露。信息伪造:攻击者通过各种手段窃取合法用户的账号信息,并利用窃取的账户信息,向其他用户发送垃圾内容或诈骗信息。

(2) 系统运营商面临的安全威胁主要来自对服务器的攻击,如 DoS 和 DDoS 攻击,攻击者大量模仿合法用户的行为请求服务,占用网络带宽和服务器资源,导致合法用户无法获得服务。同时,随着移动支付的方式越来越普及,服务器中存储了大量的个人身份信息和支付信息,这些信息一旦泄露,后果不堪设想。

(3) 通信信道的中间攻击。

目前,针对系统存在的安全性问题也采取了相应的安全措施,以保护用户数据安全。主要的安全措施有

① 数据加密技术:在即时通信系统中,通常使用两种加密方式保护数据安全:一种为存储加密,是指将一些重要的本地数据(如个人资料、通信记录等)加密保存;另一种为传输加密,是指对传输中的数据流(如账号、密码等)进行加密,通过对结点和连接加密的方式保护传输中的数据使其安全。

② 防火墙技术:防火墙技术的核心是设置通过防火墙边界的规则,对于不满足规则的访问,防火墙都会阻止其进入系统,防止造成进一步破坏。系统管理员一般通过明确禁止某些非法流量或者明确允许某些合法流量保护系统安全。

注意:基于加密技术的保密措施,一旦解密,用户数据将暴露无遗。防火墙技术也并不能对基于正常通信的"潜"信道攻击做到有效防范。下面重点介绍新的隐密技术在网络通信系统中的应用。

12.2 网络环境下的隐密通信

12.2.1 隐密通信模型

隐密通信模型如图 12-1 所示。

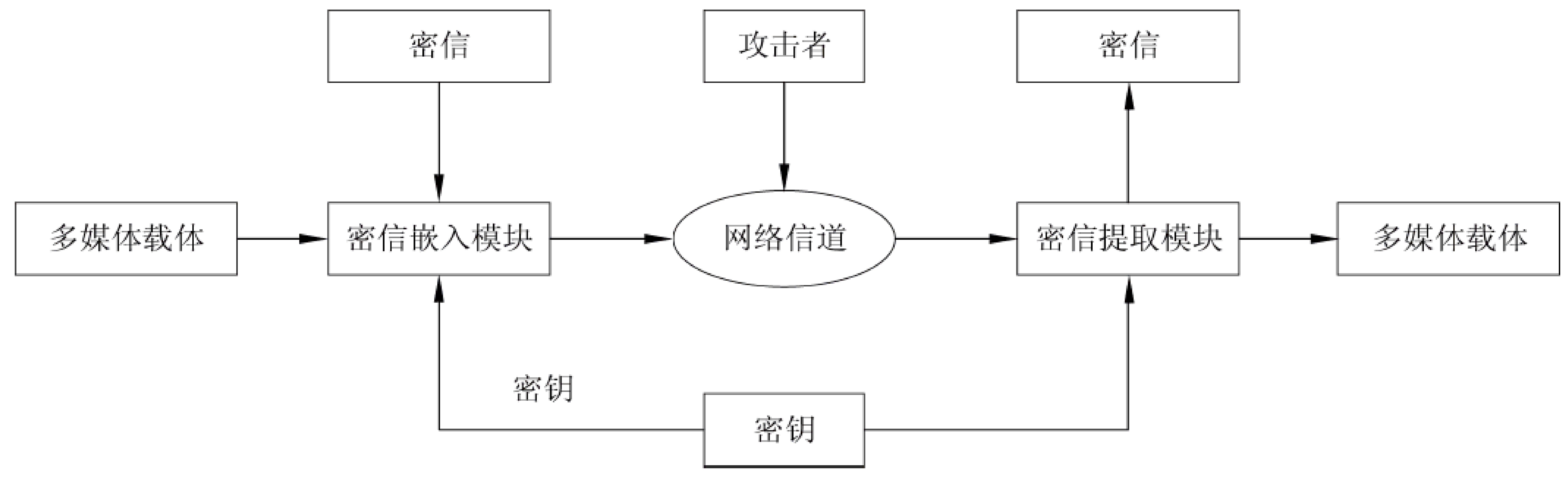


图 12-1 隐密通信模型

密信嵌入模块以载体、密信和密钥作为输入,密信可以是多种形式,常见的密信形式有文字文档、图像、音视频等。密钥可以采用公、私钥方式,其中私钥可以通过其他信道传输或与含密载体在同一信道的不同时间段传输,且隐密通信中的密钥与原始载体无关。系统根据提供的多媒体载体类型的不同,嵌密模块使用不同的密信嵌入算法将处理后的密信嵌入至多媒体载体中,生成携密载体。携密载体和原始载体的基本特征一致、感官效果相同,攻击者无法分辨出载体中是否含有秘密信息,从而大大降低密信被攻击和窃取的可能性,增强密信在网络信道中的安全性。接收到携密载体后,密信提取模块中使用与嵌入模块中对应的提取算法,结合分配的密钥提取出携密载体中隐藏的秘密信息。

12.2.2　隐密与一般通信系统的搭载模式

在网络即时通信背景中，根据秘密信息隐藏模块的应用背景，可以分为以下 3 种搭载模式。

1. 外挂式

外挂式隐密通信模块的结构如图 12-2 所示。

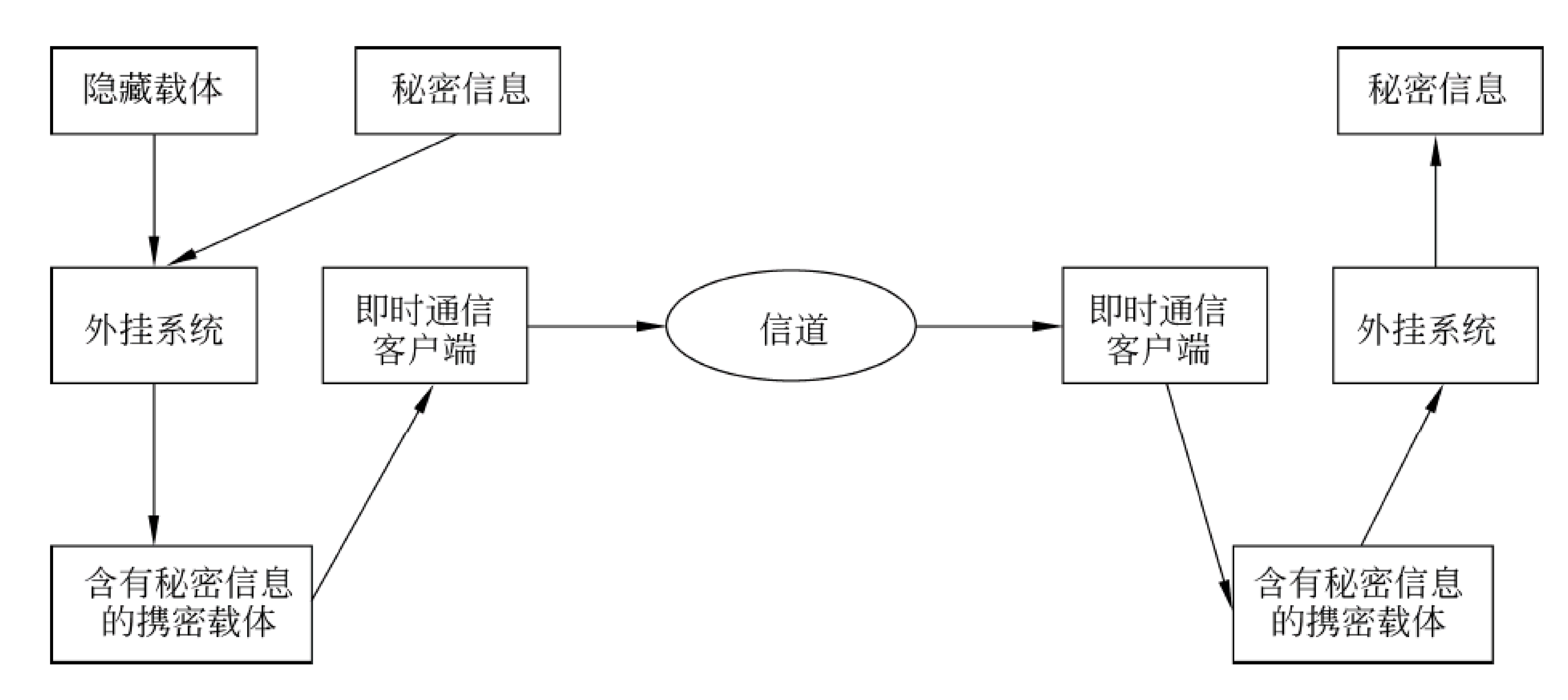


图 12-2　外挂式隐密通信模块的结构

外挂式隐密通信模块独立于即时通信客户端。在通信行为发生前，首先外挂模块根据提供的隐藏载体和秘密信息执行密信嵌入算法生成携密载体，再使用即时通信客户端将携密载体发送至网络中。接收端通信客户端接收到携密载体后，将其转发至外挂系统，外挂系统执行密信提取算法，还原出秘密信息。

外挂式隐密模块的优点是结构简单，由于外挂系统借助即时通信客户端完成通信，因此不需要在实现通信协议和结构上花费工作量。但是，其缺点也显而易见，这种方式对于非实时通信数据易于实现信息隐藏，但在实时音视频数据中的隐藏比较困难，会影响通信的实时性，并且这种方式在身份识别和认证时比较复杂。

2. 注入式

注入式隐密通信模块的结构如图 12-3 所示。

在通信客户端发送通信消息后，注入式隐密模块通过 Hook 技术将通信中的多媒体数据拦截，并传递至隐藏模块，隐藏模块执行嵌入算法将秘密信息嵌入至拦截到的数据中生成携密载体发送至网络。接收方的通信客户端在收到消息前，该通信消息首先被消息 Hook 拦截，传递至隐密模块中执行提取算法，还原出原始密信。

注入式隐密模块的优点和外挂式隐密模块相同，都依赖于第三方通信客户端，无须在实现通信协议和通信结构上花费工作量，实现相对简单。缺点是需要在系统中实现消息 Hook，相对外挂式较为复杂。

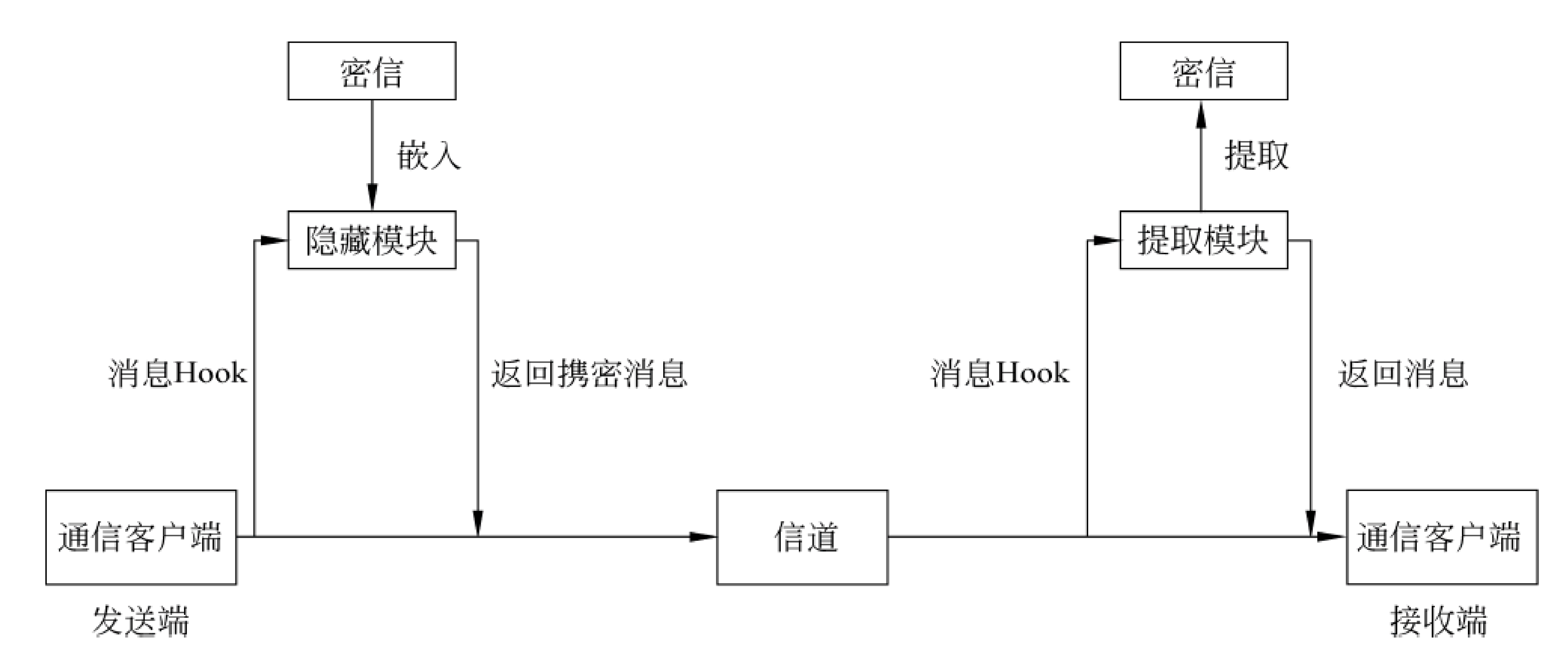


图 12-3　注入式隐密通信模块的结构

3. 伪客户端式

伪客户端式隐密通信模块的结构如图 12-4 所示。

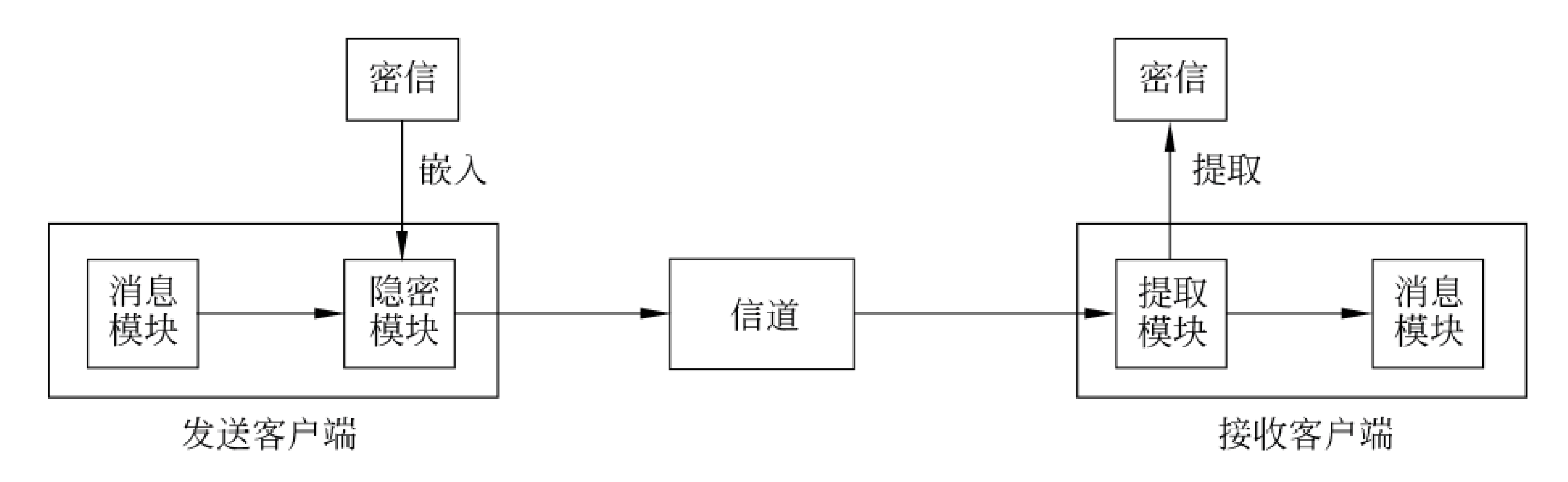
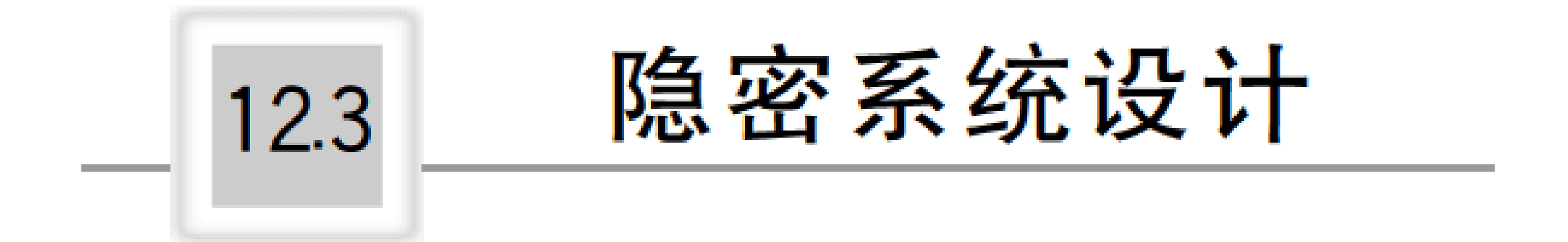


图 12-4　伪客户端式隐密通信模块的结构

在伪客户式端隐密模型中，隐密模块存在于客户端内部，与消息模块相互协调工作。进行隐密通信时，隐密模块利用消息模块产生的多媒体数据作为载体，执行嵌入算法将秘密信息嵌入至通信载体中，生成携密载体，经过网络信道发送至接收端。接收端客户端接收到携密载体后使用提取模块执行密信提取算法还原秘密信息。

由于伪客户端模式不借助第三方通信客户端，将通信模块和隐藏模块结合在一起，结构更为集中。而且通信模块和隐密模块相互协作，客户端可以实现多种方式的隐密通信，功能更加强大。但伪客户端模式的开发不仅需要实现隐密模块，还要开发网络通信模块和相关通信协议，相对前两种方式工作量较大。



12.3 隐密系统设计

12.3.1 发送端

发送方流程如图 12-5 所示。

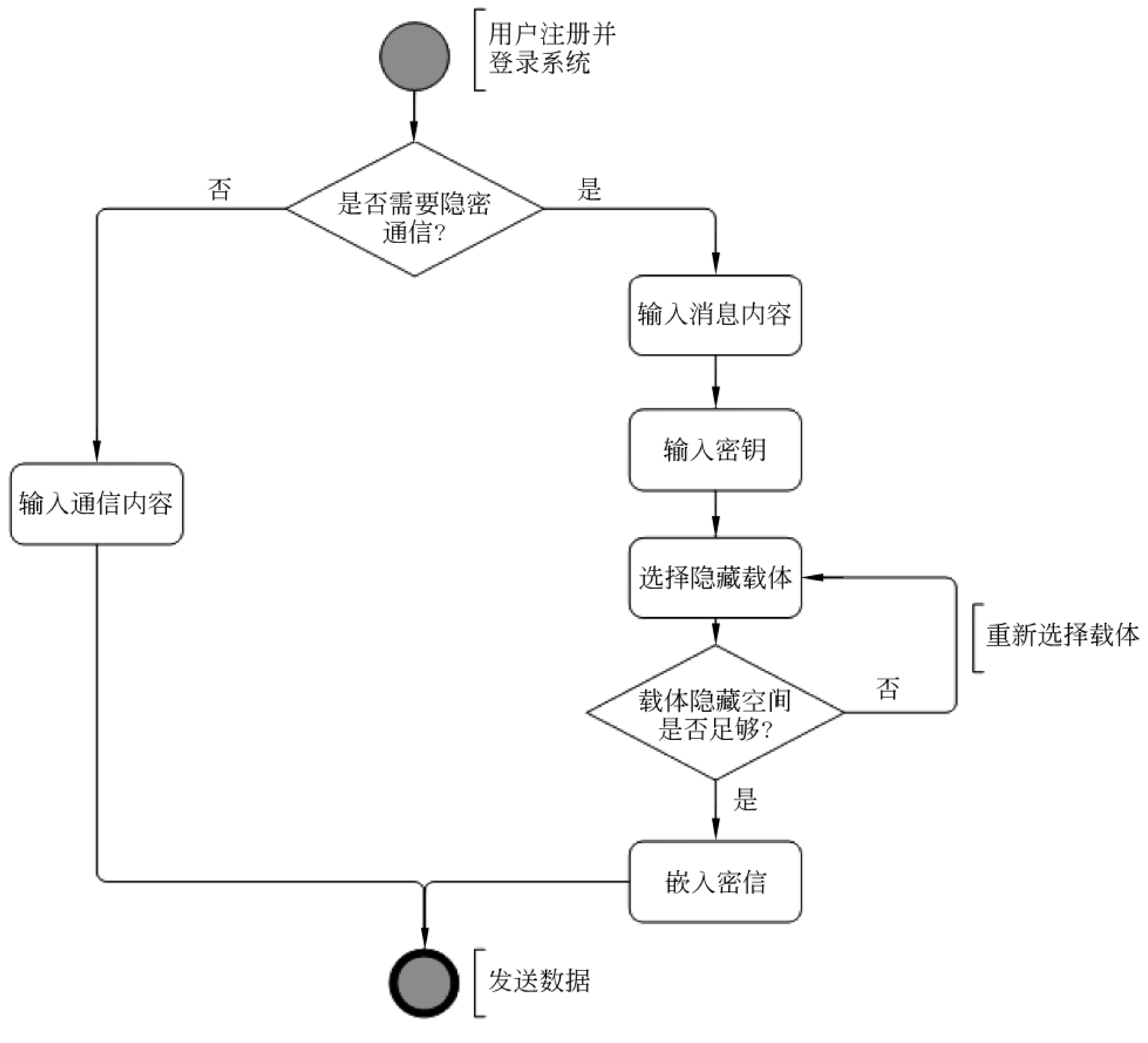


图 12-5　发送方流程

12.3.2　接收端

接收方流程如图 12-6 所示。

发送方用户在使用隐密通信功能时，需要用户提供秘密信息、输入密钥、选择合适的隐藏载体。系统执行嵌入算法后生成和正常多媒体消息相似的携密载体，发送至接收端。

接收方收到消息后，如消息中不携带秘密信息，则正常显示，否则系统执行提取算法提取出载体中的密信，再通过用户输入的密钥还原出原始秘密信息。

12.3.3　隐密通信系统架构

基于移动终端的实时隐密系统采用 C/S(Client/Server)和 P2P 相结合的架构模式，可以将系统分为客户端和服务端。系统架构图，如图 12-7 所示。

服务器属于单例模式，运行在公共网络上，为所有客户端提供服务。服务器只有 TCP 连接模块，客户端与服务器之间通过 TCP 进行通信。客户端在启动时就请求与服务器建立 TCP 长连接，连接成功后由客户端定时发送心跳包，以维持连接活跃。客户端与服务器之间的请求命令与数据交换都通过这条 TCP 连接完成。

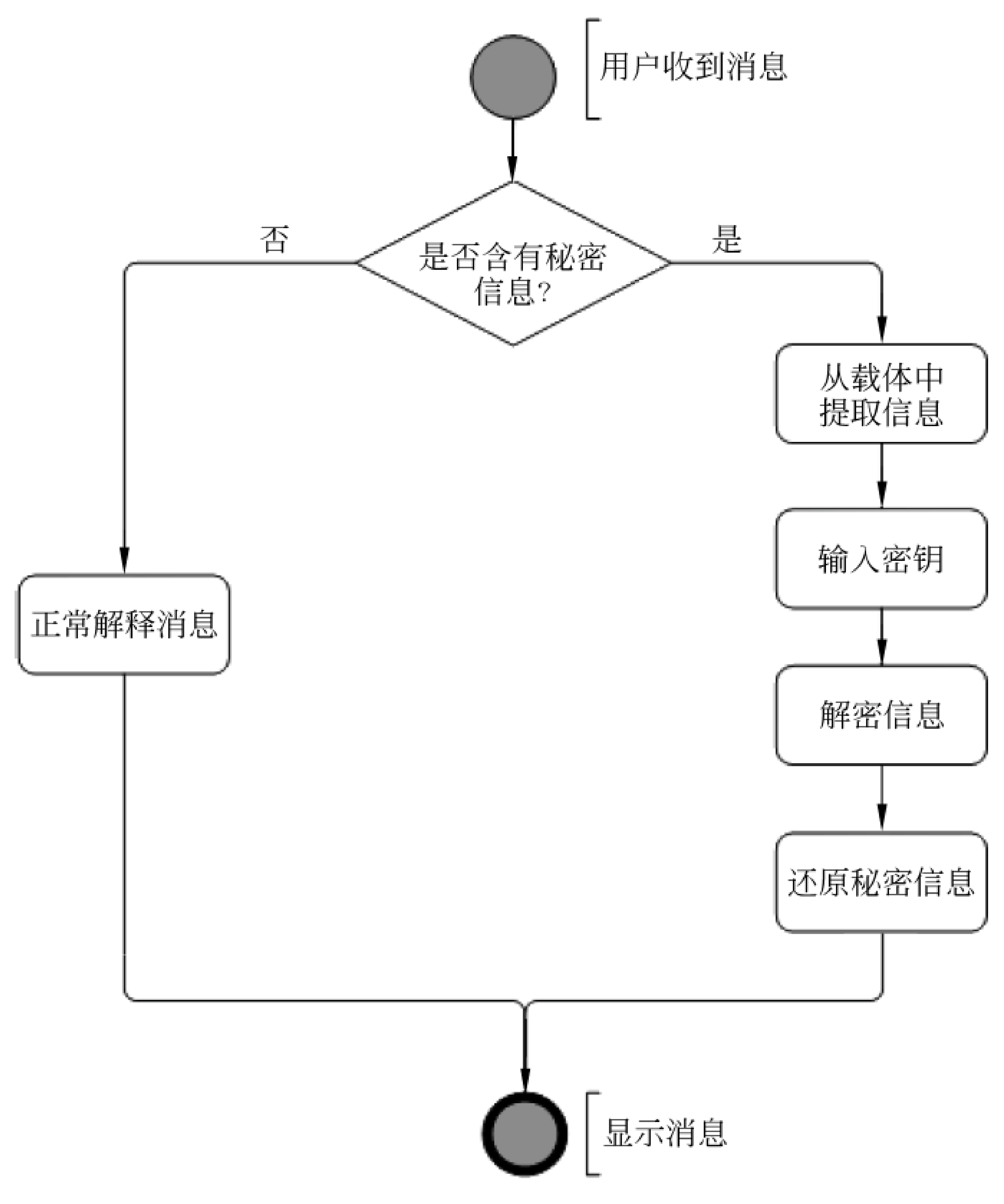


图 12-6 接收方流程

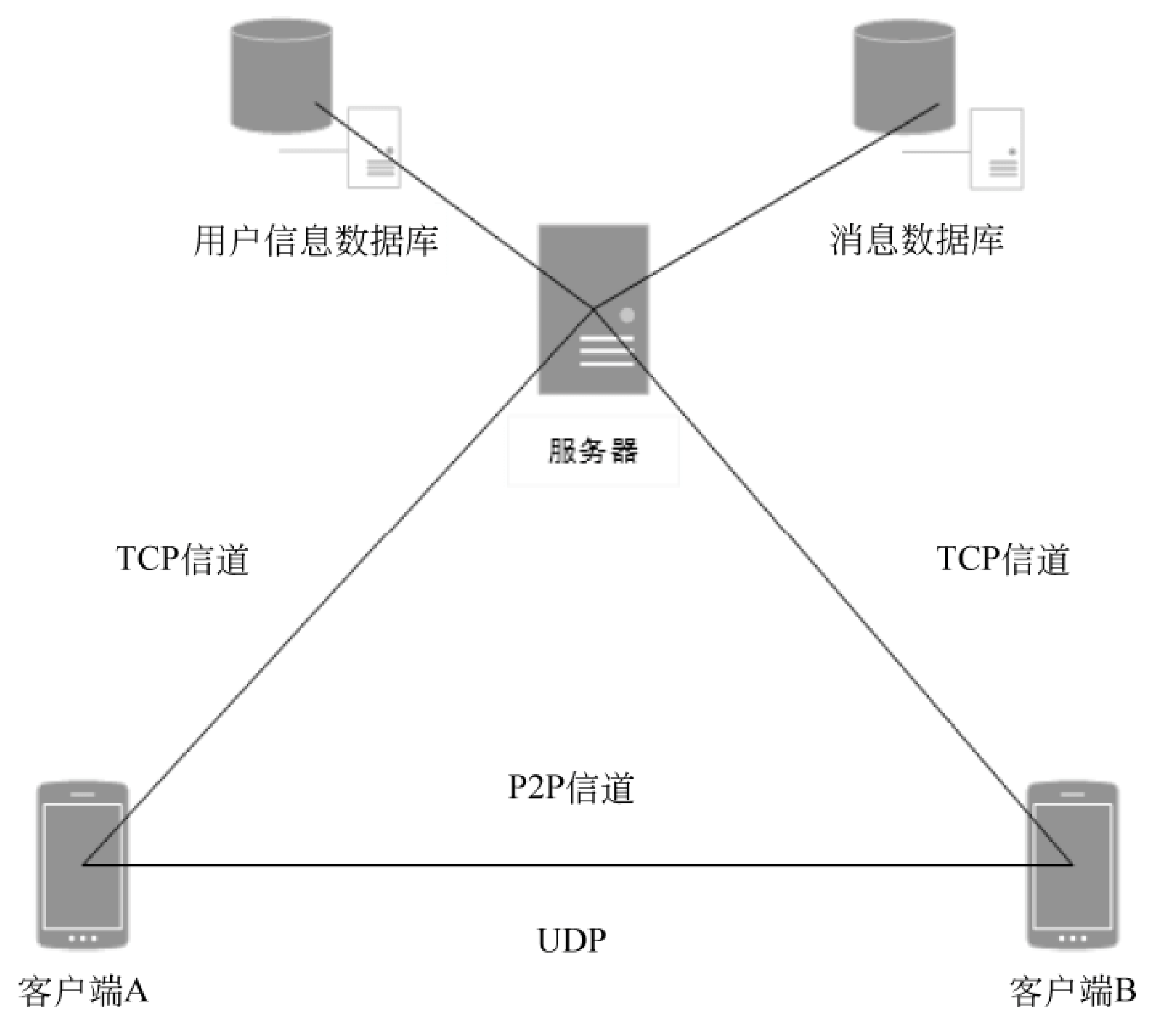


图 12-7 系统架构图

客户端运行在 Android 智能手机上，负责与用户交互、与服务器数据通信、完成信息隐藏等功能。客户端不仅需要与服务器进行数据通信，还需要与其他客户端建立 P2P 信道，因此客户端同时具有 TCP 模块和 P2P 模块。对于大数据量的通信，通信双方需要在服务器的协助下建立 P2P 信道，使用 P2P 信道进行通信。这样可以有效降低服务器的负载，减少网络拥塞。

服务端的主要功能有：

(1) 存储用户的注册信息。

(2) 在登录时验证用户信息的合法性。

(3) 存储和更新用户的好友列表。

(4) 维护用户的状态信息，如在线状态、网络地址等。

(5) 对用户发送的较短类型的消息进行转发。

(6) 协助客户端完成 NAT 穿越，建立 P2P 连接。

客户端的主要功能有：

(1) 完成用户注册功能，收集并向服务器提交合法数据。

(2) 登录系统，获取好友列表及状态信息。

(3) 管理好友列表，可添加或删除好友。

(4) 发送即时消息，消息类型可以是文本、图像、音频、视频消息。

(5) 秘密信息嵌入功能。将用户的秘密信息嵌入至选定的多媒体载体中。

(6) 秘密信息提取功能。从接收到的携密载体中提取出原始秘密信息。

12.3.4　隐密系统功能模块

基于移动终端的实时隐密通信系统分为服务端和客户端两部分，其功能模块如图 12-8 所示。

服务端相对于客户端功能较为简单，主要包含三大功能模块：用户信息管理模块、消息转发模块以及 P2P 协助模块。

用户信息管理模块主要负责管理系统用户，如存储用户个人资料、验证用户身份的合法性、维护系统用户的通信关系、记录用户的状态信息等功能，为即时通信业务提供服务。

消息转发模块主要负责将用户发送的通信消息转发至目标用户。在 C/S 通信模型中，由于通信双方都不知道对方的网络地址信息，因此需要服务器对通信消息进行转发。服务器收到通信消息后，根据通信目标的当前状态，若目标客户端与服务器之间存在活跃的 TCP 连接，则直接转发消息，否则会先将通信消息缓存至消息数据库中，等待下一次目标用户连接时再进行转发。

P2P 协助模块主要负责协助用户完成 NAT 穿越，建立客户端之间的 P2P 连接。一般情况下，用户发送的内容较短的通信消息会经过服务器转发后到达目标用户，但在用户进行大数据量、长时间的通信时，若使用服务器转发的方式，会占用大量服务器资源和网

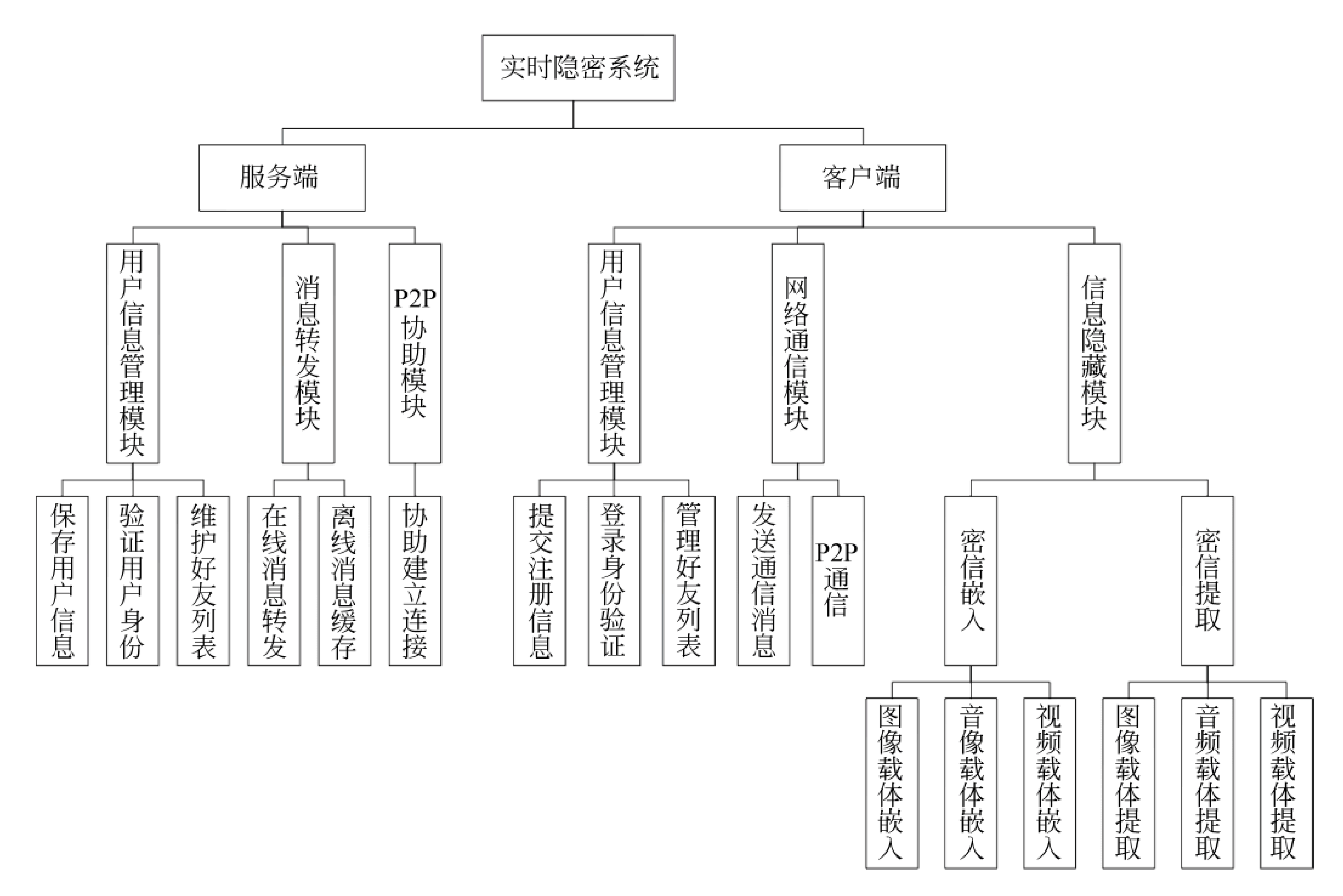


图 12-8　系统功能模块图

络带宽，因此需要使用 P2P 的通信方式。需要服务器交换双方网络地址信息，协助建立 P2P 连接。

客户端的功能相对复杂，不仅需要完成与服务器和其他终端的通信功能，还需要处理多媒体数据，并执行信息隐藏算法。客户端主要包括：用户信息管理模块、网络通信模块、信息隐藏模块。

用户信息管理模块主要为用户提供注册、登录功能，并且允许用户管理个人好友列表，可添加或删除好友。用户信息管理模块的功能需要客户端和服务器协同完成，因此服务器和客户端都有该模块，但负责的内容不同。

网络通信模块主要负责发送和接收用户的通信消息。无论是未嵌密的正常通信内容，还是隐藏后的携密载体，都需要经过网络通信模块发送至接收端。根据发送数据量的大小，系统选择不同的通信方式，较短的通信消息会通过服务器转发。大数据量的通信则会向服务器发送 P2P 请求，建立 P2P 连接。

信息隐藏模块是隐密通信的核心模块，主要负责执行信息隐藏算法，包括密信嵌入功能和密信提取功能。密信隐藏是将秘密信息隐藏至多媒体载体中的过程，根据用户提供的多媒体载体的不同类型，模块会执行不同的隐藏算法。隐藏后产生的携密载体经过网络通信模块发送至接收端。密信提取是从携密载体中提取出秘密信息的过程，根据接收到携密载体的类型，执行相应的提取算法。

12.4　系统功能模块设计

12.4.1　用户信息管理

用户信息管理模块主要负责存储管理用户注册信息、登录验证、维护用户的好友列表等功能。此模块的功能需要服务端和客户端相互配合完成，客户端提交请求和用户数据，服务器负责操作数据库并返回响应信息。该模块主要包含注册、登录、管理用户列表功能。

1. 注册功能

用户注册时，首先根据界面提示填写个人资料并单击“提交”按钮。客户端需要验证信息的完整性和合法性，对于不合法的数据，系统提示用户重新填写。验证通过后，将数据提交至服务器并等待响应。

服务器的业务层收到客户端发送的注册请求后，生成业务请求传递至 DAO 层，DAO 层为该用户创建一个用户实体并初始化用户的关系列表、消息队列等信息并存储至用户信息数据库中。操作成功后，服务器向客户端发送注册成功的响应信息。注册功能时序图如图 12-9 所示。

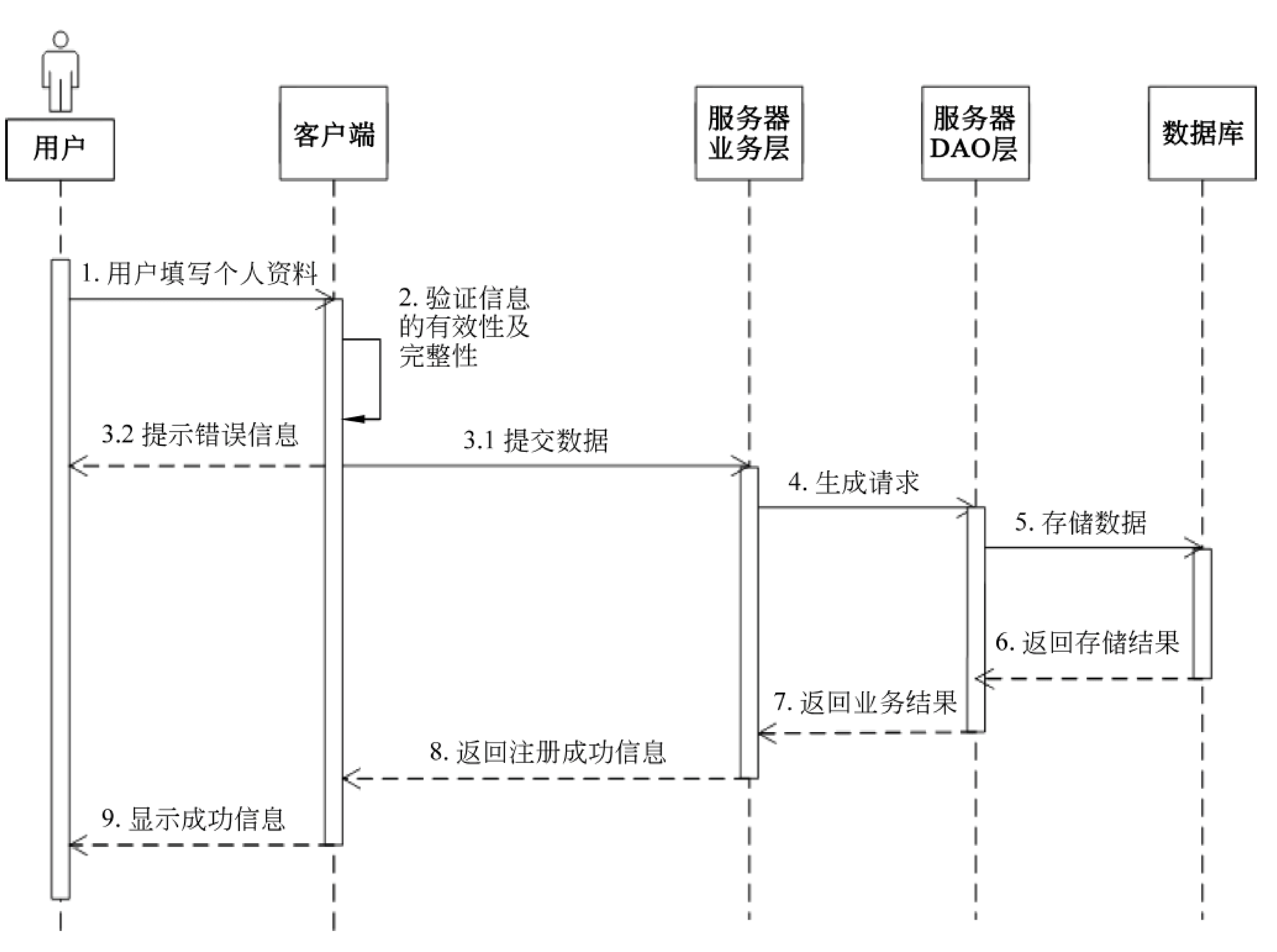


图 12-9　注册功能时序图

2. 登录功能

系统使用用户名和密码组合的方式进行登录。用户输入用户名和密码，将加密后的数据提交至服务器并等待响应。

服务器的业务层在收到数据后产生一个验证请求，并向 DAO 层请求查询数据库，DAO 层查找目标用户的身份信息。对比信息合法性后向客户端返回结果。客户端收到响应信息后，若用户身份合法，则跳转至系统的主界面，否则显示错误信息。登录功能时序图如图 12-10 所示。

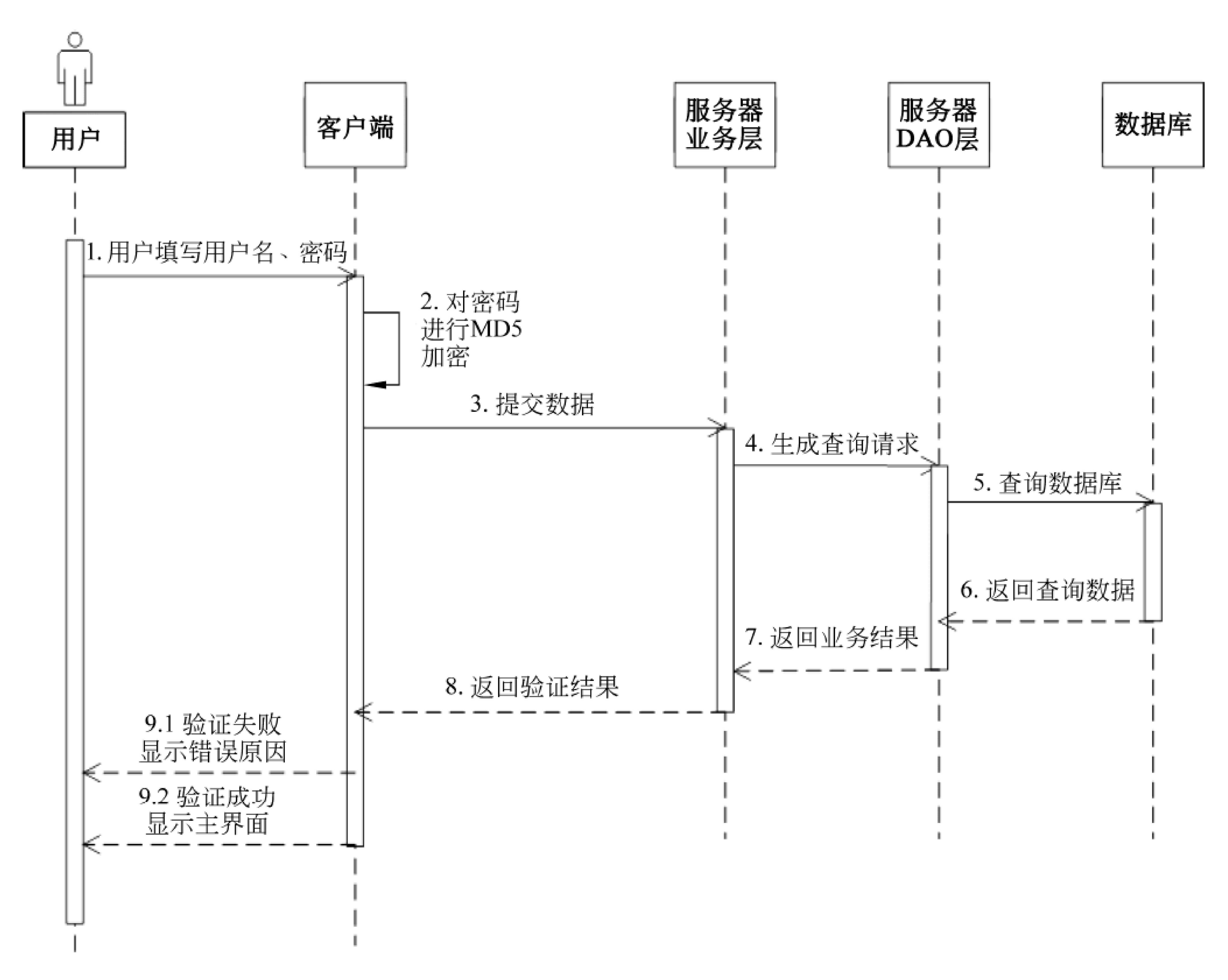


图 12-10 登录功能时序图

3. 管理用户列表功能

用户通过输入用户名的方式添加新的通信目标。首先，用户输入目标用户的用户名并单击“添加”按钮，客户端向服务器发送一条添加好友的请求。

服务器收到好友请求时，向数据库提交查询请求，查看目标用户是否存在。若目标用户不存在，则向用户返回错误信息。若目标用户存在，则向目标用户发送一条好友申请信息。目标用户同意后，服务器更新双方好友列表并向双方发送成功信息和更新后的好友列表。

管理用户列表功能时序图如图 12-11 所示。

图 12-11　管理用户列表功能时序图

12.4.2　网络通信模块

网络通信模块主要负责网络通信及数据交互的正常进行，是整个系统的基础模块。无论是系统中请求、指令，还是用户发出的通信内容，都需要通过网络通信模块发送至服务器或其他客户端。网络通信模块主要包括 TCP 连接模块和 P2P 连接模块。

1. TCP 连接模块

TCP 模块主要负责建立和维护客户端与服务器之间的 TCP 长连接。客户端与服务器都有 TCP 连接模块，系统中发送的请求、指令，用户发送较短类型的消息都会通过 TCP 连接进行传递。客户端启动时向服务器发送建立 TCP 连接的申请，双方通过三次握手协议建立 TCP 连接。连接建立后服务器会保存客户端的网络地址、连接状态等信息。由于 TCP 连接在一段时间内没有数据通信时会被释放，因此为了保持连接活跃，客户端在运行时需要向服务器定时发送心跳包，心跳包长度很小，并且除了保持连接活跃，

没有其他作用。用户退出主界面，客户端进入后台运行时，TCP 连接依旧保持活跃，客户端可以正常接收消息并显示在通知栏。用户单击“退出”按钮确认退出后，客户端向服务器发送终止连接请求，双方通过 4 次挥手协议结束连接。

2. P2P 连接模块

客户端不仅有和服务器通信的 TCP 模块，还有与其他客户端通信的 P2P 连接模块。在客户端需要进行长时间、大数据量的数据通信时，需要在服务器的协助下建立基于 UDP 的 P2P 信道。P2P 信道的建立需要客户端的 P2P 通信模块和服务器的 P2P 协助模块。

由于通信双方的网络环境不同，客户端可能处于内部网络中，而 NAT 设备为了防止内部网络的广播泛滥，会阻止许多外部消息进入内部网络，双方通信时会受到 NAT 设备的阻碍，因此建立 P2P 连接首先需要穿越 NAT 设备。客户端 A 与客户端 B 建立 P2P 连接的过程如下。

- 客户端 A 首先通过与服务器的 TCP 连接向服务器发送 P2P 协助请求。
- 客户端 A 通过 P2P 端口向服务器的 P2P 端口发送数据包，让服务器获取客户端 A 中 P2P 端口映射至外界的网络地址。
- 服务器将客户端 A 建立 P2P 连接的请求和主机 A 中 P2P 端口的对外地址通过 TCP 连接转发给客户端 B。
- 客户端 B 收到建立连接的请求后，使用 P2P 端口向服务器发送接收连接的数据包，让服务器获得客户端 B 中 P2P 端口的对外网络地址。
- 客户端 B 通过 P2P 端口向客户端 A 中 P2P 端口地址发送数据包，让客户端 B 所在的 NAT 设备记录客户端 A 的地址。
- 服务器将客户端 B 中 P2P 端口的信息转发给客户端 A。
- 客户端 A 通过 P2P 端口向客户端 B 的 P2P 端口发送数据包，由于客户端 B 所在的 NAT 设备已经记录了客户端 A 的 P2P 端口地址，所以该数据包能成功穿越 NAT 设备，到达客户端 B，同时客户端 A 所在的 NAT 设备也会记录客户端 B 的地址信息。
- 客户端 B 收到客户端 A 发送的数据包后，向客户端 A 发送确认数据包。客户端 A 所在的 NAT 设备已经记录了客户端 B 的地址信息，因此该确认包能正常到达客户端 A。
- 客户端 A 收到确认包后向客户端 B 发送确认包。

客户端 A 能够正确收到客户端 B 发送的确认包，说明客户端 B 到客户端 A 的 P2P 信道成功建立，客户端 B 能够正确收到客户端 A 发送的确认包，则说明客户端 A 到客户端 B 的 P2P 信道成功建立，如图 12-12 所示。

3. 消息转发模块

消息转发模块是服务端的功能模块，负责将客户端发送的短消息转发至目标接收端。

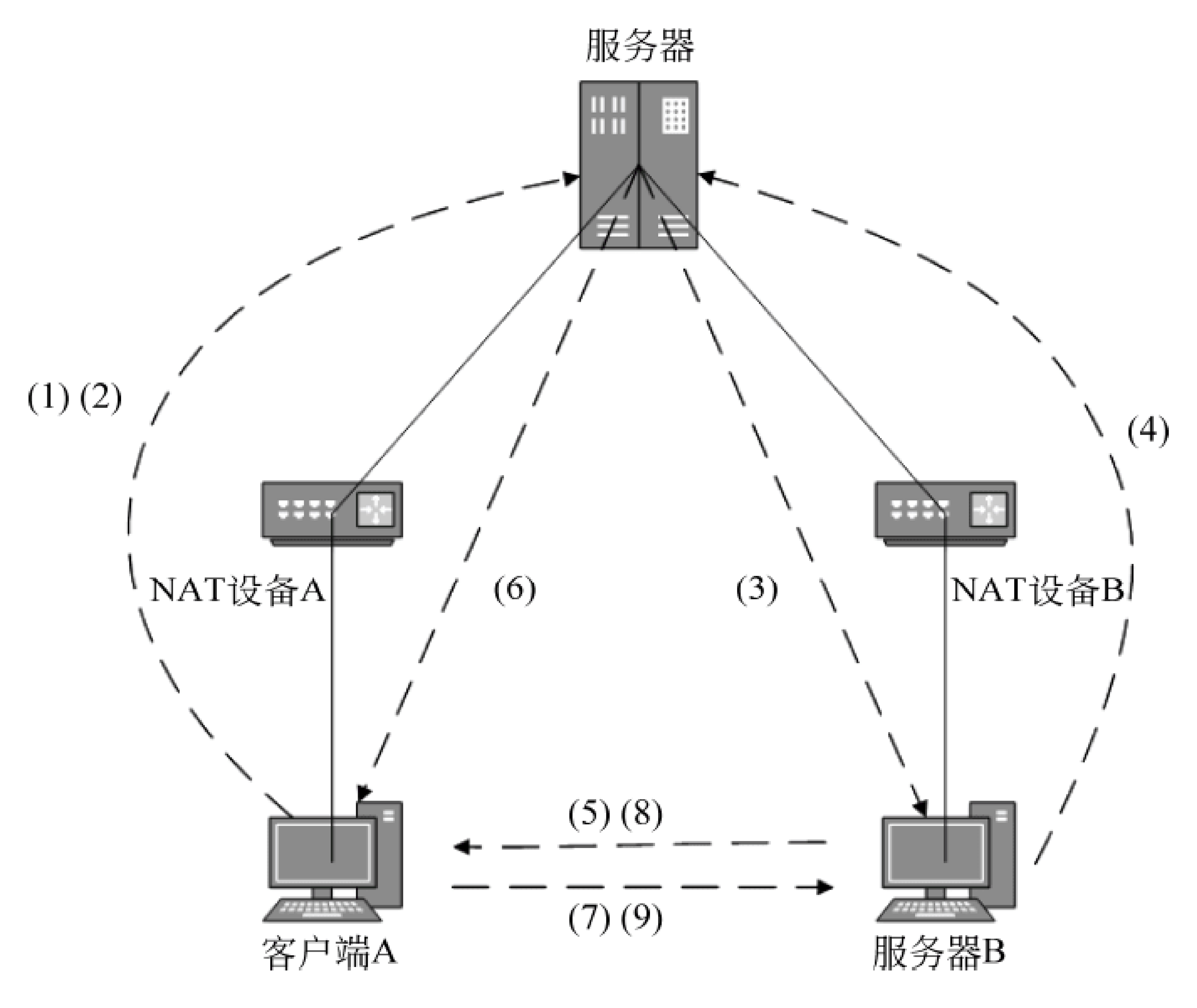


图 12-12　P2P 连接过程

服务器与多个客户端维持连接，需要维护一张用户状态表，用于存储该用户的网络地址、连接状态等信息。

服务器收到一个通信消息后，首先解析该数据包，得到通信目标用户的 ID，再使用目标用户 ID 查询状态表找出目标用户的连接状态。若服务器与该用户的连接存在，则获取该用户的 TCP 连接实例，通过该连接实例将该通信消息转发至目标客户端，否则，服务器就将通信消息暂存至消息数据库中，等目标用户建立连接后，再从消息数据库中读取该消息，转发至客户端，如图 12-13 所示。

12.4.3　信息隐藏模块

信息隐藏模块是整个隐密通信的核心模块，主要在客户端执行信息隐藏算法，满足用户的隐密通信功能。该模块分为密信嵌入模块和密信提取模块两部分。

密信嵌入模块属于通信中发送方的功能模块，主要负责将秘密信息隐藏至选定的多媒体载体中。用户嵌入秘密信息的过程如下。

(1) 输入秘密信息内容。密信可以是文字、图片、文件等任意格式。

(2) 输入密钥。系统由密钥生成密信置乱参数和位置信息置乱参数，使用密信置乱参数对密信进行置乱操作。

(3) 系统对置乱后的密信进行编码，产生密信的二进制序列。

(4) 用户选择隐藏载体，系统可以使用图像载体、音频载体和视频载体。

(5) 对选定载体进行内容特征分析，找出适合隐藏、特征明显的区域。

(6) 将二进制序列嵌入至特征明显的区域，并生成位置信息。

(7) 使用密信参数对位置信息进行置乱。

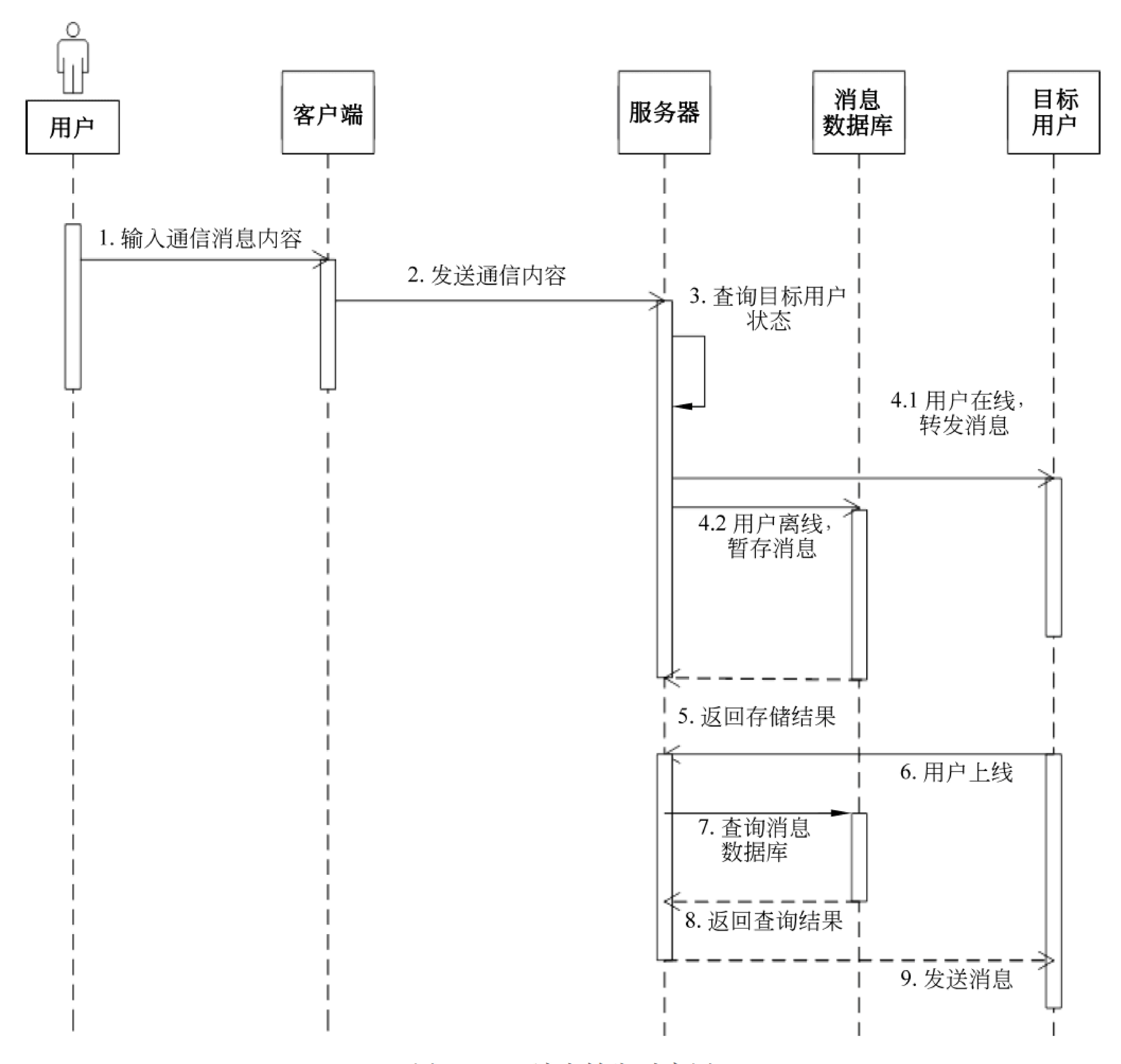


图 12-13　消息转发时序图

完成密信嵌入过程后，会产生一个与原始载体特征相似的携密载体以及一组置乱后的位置信息，系统分别将携密载体和位置信息通过网络通信模块发送至接收端。

密信提取模块属于隐密通信中接收方的功能模块，主要负责利用位置信息提取出携密载体中的秘密信息，如图 12-14 所示。提取秘密信息的过程如下。

(1) 接收方收到携密载体和置乱后的秘密信息。

(2) 输入密钥。根据密钥生成密信置乱参数和位置信息置乱参数。使用位置信息置乱系数对置乱后的位置信息进行逆置乱操作，得到原始位置信息。

(3) 对携密载体进行内容特征分析，结合位置信息找到密信嵌入的位置。

(4) 从隐藏位置提取出秘密信息的二进制序列，并将二进制序列还原密信。

(5) 使用密信置乱参数对密信进行逆置乱，得到原始的秘密信息。

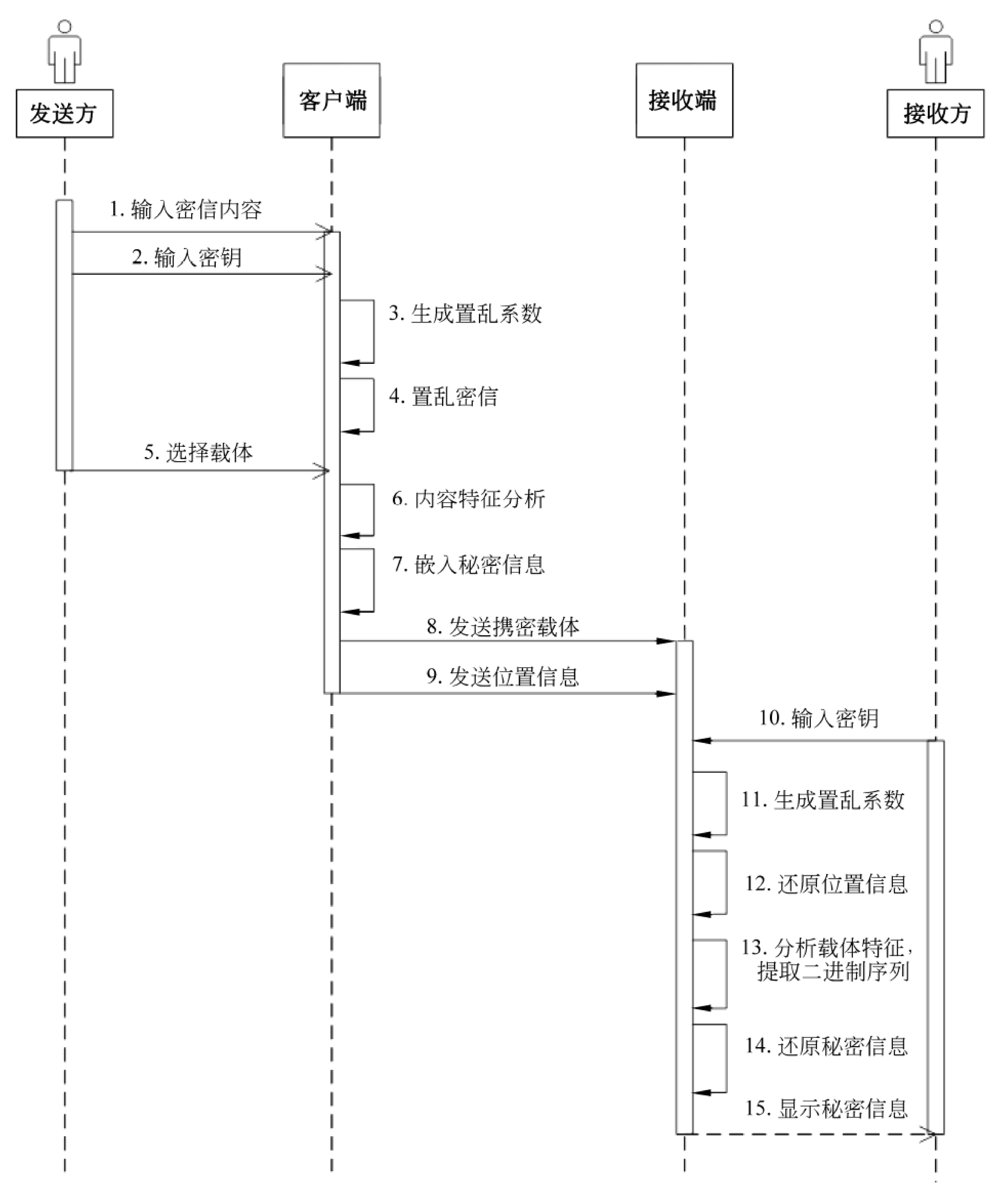


图 12-14　信息隐藏时序图

12.5 数据结构设计

基于移动终端的实时隐密系统的业务中使用了许多数据结构，本节分析和设计了系统中各个功能模块中使用的数据结构。

12.5.1 用户信息管理模块

1. 注册功能

用户注册时需要向服务器提交个人身份信息,注册为系统的合法用户。注册功能数据结构字段表见表 12-1。

表 12-1 注册功能数据结构字段表

字 段 名	字 段 意 义
user_name	用户名,用户登录时需要使用用户名登录系统
password	密码,用户登录时使用密码验证身份
phone_number	手机号码,用于发送验证码信息
email_address	电子邮箱,用于找回密码的一种途径

注册功能使用的数据结构为

```
typedef struct {
    String user_name;          //字符串,长度不超过 64 个字符
    String password;           //字符串,密码为经过 MD5 加密后的密文
    String phone_number;       //字符串,手机号码为经过正则表达式验证后的合法号码
    String email_address;      //字符串,邮箱地址为经过正则表达式验证后的合法地址
} REGISTER_PACKAGE
```

2. 登录功能

用户登录系统时需要向系统提交自己的身份信息。登录功能数据结构字段表见表 12-2。

表 12-2 登录功能数据结构字段表

字 段 名	字 段 意 义
user_name	用户名,用户在注册时填写的身份名称
password	密码,用户在注册时填写的身份验证信息

登录功能使用的数据结构为

```
typedef struct {
    String user_name;          //字符串,长度不超过 64 个字符
    String password;           //字符串,密码为经过 MD5 加密后的密文
} LOGIN_PACKAGE
```

3. 管理好友列表

管理好友列表功能包括添加好友和删除好友,需要用户向服务器发出请求,客户端需要向服务器提交的数据字段见表 12-3。

表 12-3　管理好友功能数据结构字段表

字 段 名	字 段 意 义
user_name	用户名，发出申请的用户身份
target_user_name	目标用户名，需要添加或删除的目标用户的身份
operation	操作目的，说明用户是需要添加好友，还是删除好友
result	操作结果，说明服务器或用户返回的结果

管理好友列表使用的数据结构为

```
typedef struct {
    String user_name;           //字符串，长度不超过 64 个字符
    String target_user_name;    //字符串，密码为经过 MD5 加密后的密文
    byte operation;             //字节型，0 表示添加好友，1 表示删除好友
    boolean result;             //布尔型，true 表示操作成功，false 表示操作失败
} FRIDMANAGE_PACKAGE
```

12.5.2　网络通信模块

网络通信模块使用的数据结构主要是通信消息。通信消息数据结构字段表见表 12-4。

表 12-4　通信消息数据结构字段表

字 段 名	字 段 意 义
source_user_name	发送方用户名，消息发送方的用户身份
target_user_name	接收方用户名，消息接收方的用户身份
send_time	消息发送时间，记录消息发送的时间
message_type	消息类型，描述消息的类型(如文字、图片、语音、视频等)
message_extension	消息内容扩展名，描述非文字消息的内容格式
message_content	消息内容，通信消息的具体内容

通信消息使用数据结构为

```
typedef struct {
    String source_user_name;    //字符串，长度不超过 64 个字符
    String target_user_name;    //字符串，长度不超过 64 个字符
    Date send_time;             //日期类型，表示消息发送的日期和时间
    byte message_type;          //布尔型，true 表示操作成功，false 表示操作失败
    String message_extension;   //字符串，表示非文字类型消息的内容格式
    byte[] message_content;     //字节数组，存放具体的消息内容
} MESSAGE_PACKAGE
```

12.5.3 信息隐藏模块

1. 秘密信息

秘密信息使用的数据结构主要是对待嵌入的密信进行存储。密信数据结构字段表见表 12-5。

表 12-5 密信数据结构字段表

字 段 名	字 段 意 义
message_type	密信类型,描述密信的消息类型(如文字、图像、文件等)
message_extension	密信扩展名,对于非文字消息,需要指定密信的格式,接收端根据格式还原密信文件
message_length	密信长度,描述秘密信息的长度
message_content	密信内容,秘密信息的实际内容

秘密信息使用的数据结构为

```
typedef struct {
    byte message_type;              //字节型,0 表示文字消息,1 表示文件消息
    String message_extension;       //字符串,表示非文字类型消息的内容格式
    long message_length;            //长整数型,表示密信内容所占的字节数
    byte[] message_content;         //字节数组,存放具体的密信内容
} MSG_PACKAGE
```

2. 隐藏载体

隐藏载体所使用数据结构主要描述原始载体或携密载体的信息,应包含的数据字段见表 12-6。

表 12-6 载体数据结构字段表

字 段 名	字 段 意 义
covert_type	载体类型,描述载体的类型(如图像、音频、视频等)
covert_extension	载体扩展名,用于描述多媒体载体的格式信息
covert_length	载体长度,描述多媒体载体的长度
covert_content	载体内容,多媒体载体的实际内容

隐藏载体使用的数据结构为

```
typedef struct {
    byte covert_type;               //字节型,0 为图像载体,1 音频载体,2 为视频载体
    String covert_extension;        //字符串,表示多媒体载体的内容格式
    long covert_length;             //长整数型,表示载体内容所占的字节数
    byte[] covert_content;          //字节数组,存放具体载体的内容数据
```

```
} COVERT_PACKAGE
```

12.5.4　数据库设计

本系统中的数据库主要分为两部分：客户端数据库和服务器数据库。

客户端数据库通过 Android 系统提供的 SQLite 数据库实现。SQLite 是一种可靠的轻量级关系型数据库。客户端中数据库主要存储的是与其他用户的消息记录，可以让用户查询以前通信的消息内容。客户端数据库只需要存储通信记录，只有一张通信记录表，记录表中的各个字段见表 12-7。

表 12-7　客户端通信消息表

字 段 名	字 段 意 义
ID	整数型，该数据表的主键
SEND_USER	字符串，消息的发送者
RECEIVE_USER	字符串，消息的接收者
RECEIVE_DATE	日期类型，消息发送的时间
MESSAGE_TYPE	整数型，表示收到消息的类型
MESSAGE_FILE_PATH	字符串，若消息为文字消息，则该字段为空，反之该字段表示消息文件在文件系统中的绝对路径
MESSAGE_CONTENT	字符串，若消息为文字消息，则该字段保存文字消息的内容，反之该字段为空
IS_MESSAGE_READ	布尔类型，表示该消息是否被阅读

服务器数据库主要分为两部分：用户信息数据库和消息数据库。用户信息数据库主要存储用户的个人资料、身份信息、每个用户的好友列表等信息，分为用户信息表、状态信息表、好友关系表。

用户信息表存储用户的个人资料和身份信息，见表 12-8。

表 12-8　用户信息表

字 段 名	字 段 意 义
ID	整数型，该数据表的主键
USER_NAME	字符串，表示用户的用户名
USER_PWD	字符串，表示用户的密码
USER_PHONE_NUMBER	字符串，表示用户的电话号码
USER_EMAIL_ADDRESS	字符串，表示用户的邮箱地址

状态信息表存储用户的状态信息，见表 12-9。

表 12-9 状态信息表

字 段 名	字 段 意 义
ID	整数型,外键,是用户信息表的主键
USER_STATE	布尔型,表示用户和服务器的连接状态
USER_ADDRESS	字符串,存储用户的网络地址,若用户离线,则该字段为空
HAS_MESSAGE	布尔型,表示用户是否存在离线消息

好友关系表表示当前用户有哪些好友,用户量增多时关系表的记录数会大量增加,因此系统对每个用户都需要创建一个好友关系,见表 12-10。

表 12-10 好友关系表

字 段 名	字 段 意 义
ID	整数型,当前数据表的主键
USER_ID	整数型,外键,表示当前用户的好友 ID
USER_STATE	布尔型,表示当前好友的连接状态

消息数据库主要存储用户发送的消息,当用户通信消息的目标用户不在线时,服务器就将该消息存进服务器。消息数据表见表 12-11。

表 12-11 消息数据表

字 段 名	字 段 意 义
ID	整数型,当前数据表的主键
MESSAGE_SEND_USER	整数型,外键,表示当前用户的好友 ID
MESSAGE_RECEIVE_USER	布尔型,表示当前好友的连接状态
MESSAGE_RECEIVE_DATE	日期类型,消息的发送日期
MESSAGE_TYPE	整数型,表示当前消息的类型
MESSAGE_FILE_PATH	字符串,若消息是文字消息,则该字段为空,反之该字段表示消息文件在文件系统中的绝对路径
MESSAGE_CONTENT	字符串,若消息为文字消息,则该字段保存文字消息的内容,反之该字段为空

参 考 文 献

[1] Simmons G J. The prisoners' problem and the subliminalchannel[J]. Advances in Cryptology, 1984,1: 51-67.

[2] 何大可,唐小虎.现代密码学[M].北京:人民邮电出版社,2009.

[3] AhlswedeR, Csiszár I. Common randomness in information theory and cryptography Ⅱ-Secret sharing [J]. IEEE Transactions on Information Theory, 1993,39(4): 1121-1132.

[4] Ahlswede R,Dueck G. Identification in the presence of feedback—a discovery of new capacity formulas[J]. IEEE Transactions on Information Theory,1989,35(1): 30-36.

[5] Csiszár I and Körner J. Information Theory: Coding theorems for Discrete memoryless Systems [M]. Pittsburgh: Academic Press, 1981.

[6] Moulin P, O'Sulliovan J A. Information-theoretic analysis of information hiding[J]. IEEE Transactions on Information Theory,2003,49(3): 563-593.

[7] Steinberg Y, Merhav N. Indentification in the presence of side information with application towatermarking[J]. IEEE Transactions on Information Theory,2001,47(1): 1410-1422.

[8] Yeung R W. A First Course in InformationTheory[J]. IEEE Transactions on Information Theory, 2003,49(7): 1869-1869.

[9] Ahlswede R, Csiszár I. Common randomness in information theory and cryptographyⅡ[J]. Piscataway: IEEE Transactions on Information Theory,1993,39(4): 1121-1132.

[10] Csiszár I, Körner J. Information Theory: Coding theorems for Discrete memoryless Systems[M]. Pittsburgh: Academic Press, 1981.

[11] TRI V L. Information hiding [D]. Florida: Florida State University College of Arts and Sciences, 2004: 22-47.

[12] 杨世勇,吴晓丽,岳安军,等. 一种新的基于图像内容特征的顽健水印[N].通信学报,2005(6): 37-41.

[13] Petitcolas F A P, Anderson R J, Kuhn M G. Information hiding-a survey[J]. Proceedings of the IEEE,1999,87(7): 1062-1078.

[14] Anderson R J, Petitcolas F AP. On the Limits of Steganography[J]. IEEE Journal of Selected Areas in Communications, 1998,16(4) : 474-481.

[15] Fridrich J, Goljan M. Practical Steganalysis of digital images: state of the art[J]. Proceedings of SPIE—The International Society for Optical Engineering, 2002(6): 1-13.

[16] Swanson M D, Kobayashi M and Tewfik AH. Multimedia data embedding and watermarking techniques[J]. Proceedings of the IEEE, 1998,86(6): 1064-1087.

[17] Memon N. Authentication techniques for multimedia content[J]. Proceedings of SPIE—The International Society for Optical Engineering,1998(1): 412-422.

[18] Paskin N. Towards unique identifiers[J]. Proceedings of the IEEE, 1999,87(7): 1208-1227.

[19] Friedman G L. The trustworthy digital camera: Restoring credibility to the photographicimage[J]. IEEE Transactions on Consumer Electronics, 1993,39(4): 905-910.

[20] Wong P W, Memon N. Secret and public key image watermarking schemes for image authentication

and ownership verification[J]. IEEE Transactions on Image Processing, 2001,10(10): 1593-1601.

[21] Kundur D, Hatzinakos D. Digital watermarking for telltale tamper proofing and authentication[J]. Proceedings of the IEEE, 1999,87(7): 1167-1180.

[22] Wu M, Liu B. Watermarking for image authentication[J]. IEEE International Conference on Image Processing, 1998,2: 437-441.

[23] Hu Yongjian, Kwong sam. Wavelet domain adaptive visible watermark[J]. IEEE Electronics Letters, 2001,37(20): 1219-1220.

[24] Yeung M M, Mintzer F C, Braudaway G W. Digital Watermarking for High Quality Imaging[J]. Proceeding of IEEE First Workshop on Multimedia Signal Processing, 1997(6): 357-362.

[25] Meng J, Chang S F. Embedding visible video watermarking in the compressed domain[J]. Proceeding of IEEE, 1998(1): 474-477.

[26] Magerlein K A, Braudaway G W, Mintzer F C. Protecting publicly-available images with a visible image watermark[J]. Proceedings of SPIE—The International Society for Optical Engineering, 1996(5): 126-132.

[27] Kankanhalli M S, Ramakrishnan K R. Adaptive visible watermarking of images[J]. Proc. ICMCS'99, 1999(6): 568-573.

[28] Mohanty S P, Ramakrishnan K R, Kankanhalli M S. A DCT domain visible watermarking technique for images[J/OL]. (2002-10-5)[2019-02-06]. https://www.researchgate.net/publication/2536682_An_Adaptive_DCT_Domain_Visible_Waterm arking_Technique_for_Protection_of_Publicly_Available_Images.

[29] Cox I J, Kilian J, Leighton F T. Secure spread spectrum watermarking for multimedia[J]. IEEE Transactions on Image Processing, 1997,6(12): 1674-1687.

[30] Moulin P, Ivanovic A. Non-additive Gaussian watermarking and its application to wavelet-based image watermarking[J]. Proceeding of IEEE International Conference on Image Processing, 2002,3: 473-476.

[31] Barni M, Bartolini F, Cappellini V. A DCT-domain system for robust image watermarking[J]. Signal Processing, 1998,66(3): 357-372.

[32] Nikolaidis N, Pitas I. Robust image watermarking in the spatial domain[J], Signal Processing, 1998,66(3): 385-403.

[33] Zhu Wenwu, Xiong Zixiang, Zhang Ya-Qin. Multi-resolution watermarking for images and video [J]. IEEE Transactions on Circuits and Systems for Video Technology, 1999,9(4): 545-550.

[34] Xia X G, Boncelet C G, Arce G R. Wavelet transform based watermark for digital images[J]. Optics Express, 1998,3(12): 497-511.

[35] Kundur D, Hatzinakos D A. robust digital image watermarking method using wavelet based fusion [J]. IEEE International Conference on Image Processing, 1997,1: 544-547.

[36] Simmons G J. The prisoners' problem and the subliminal channel[J]. Workshop on Communications Security (CRYPTO'83), 1983,1: 51-67.

[37] Gladney H M, Mintzer F C, Schiattarella F. Safeguarding digital library contents and users: digital images of treasured antiquities[J/OL]. [2019-02-17]. http://www.dlib.org/dlib/july97/vatican/07gladney.html. 1997.

[38] Macq, Benoit. Special issue on identification and protection of Multimedia Information[J]. Processing of the IEEE, 1999,87(7): 1058-1061.

[39] Caronni G. Assuring ownership rights for digital images[J]. Berlin: Vieweg Publishing Company Germany, 1995,5: 251-263.

[40] Caronni G. Ermitteln unauthorisierter Verteiler von maschinenlesbaren Daten[J]. Technical report, 1993,97: 423-436.

[41] Tirkel A, van Schynel G R, Ho W, etc. Electronic watermark[J]. Proceedings DICTA, 1993,7: 666-672.

[42] Hernandez J J, Perez-GonzalezF, Rodriguez J. M. Performance analysis of a 2-Dmultipulse amplitude modulation scheme for data hiding and watermarking still images[J]. IEEE Journal on Selected Areas of Communications, 1998,16(4): 510-524.

[43] Wolfgang R B, Delp E J. A watermark for digital images[J]. Proceeding IEEE on Image Processing, 1996(3): 219-222.

[44] Delaigie J F, De Vleeschouwer D, Macq B. Low cost perceptive digital picture watermarking method[J]. Proceedings of SPIE—The International Society for Optical, 1997(1): 153-167.

[45] Macq B, Delaigie J F, De Vleeschouwer D. Digitalwatermarking[M]. San Jose: SPIE, 1996: 99-110.

[46] Tirkel A Z, Osborn C F, Hall T E. Image and watermark registration[J]. Signal Processing, 1998,66(3): 373-383.

[47] Kutter M, Jordan F, Bossen F. Digital signature of color images using amplitude modulation[J]. Journal of Electronic Imaging, 1998,7(2): 326-332.

[48] Kutter M, Winkler S. A vision-based masking model for spread spectrum image watermarking[J]. IEEE Transaction Image Processing, 2002,11(1): 16-25.

[49] Chen B. Design analysis of digital watermarking information embedding and data hiding sustems [D]. Cambridge: Cambridge University, 2000.

[50] Rongen P M J, Maes M. van Overveld C W A M. Digital image watermarking by salient point modification: practical results[J]. Proceedings of SPIE—The International Society for Optiacl, 1999,1: 273-282.

[51] Maes M, Overveld C W A M. Digital watermarking by geometric warping[J]. Proceedings IEEE International Conference on Image Processing, 1998,1: 424-446.

[52] Bas P, Chassery J M, Davoine F. Using the fractal code to watermark images[J]. Proceedings IEEE International Conference on Image Processing, 1998,1: 469-473.

[53] Nikolaidis A, Pitas I. Region-based image watermarking[J]. IEEE Transaction on Image Processing, 2001,10(11): 1726-1740.

[54] Nikolaidis A, Pitas I. Robust watermarking of facial images based on salient geometric patternmatching[J]. IEEE Transaction on Multimedia, 2000,2(3): 172-184.

[55] Koch E, Zhao J. Towards robust and hidden image copyright labeling[J]. IEEE Workshop on Nonlinear Signal and Image Processing, 1995,6: 123-132.

[56] Tao B, Dickinson B. Adaptive watermarking in the DCTdomain[J]. Proceedings IEEE International Conference on Image Processing, 1996,9: 153-156.

[57] Fridrich J. Image watermarking for tamper detection[J]. Proceedings IEEE International Conference on Image Processing, 1998,10: 404-408.

[58] Wenjun Zeng. A Statistical Watermark Detection Technique Without Using Original Image for Resolving Rightful Ownerships of Digital Images[J]. IEEE Transaction on Image Processing, 1999,8

(11): 1534-1547.
[59] Podilchuk C I, Zeng W. Image-adaptive watermarking using visual models[J]. IEEE Journal on selected areas in communication, 1998,16(4): 525-539.
[60] Podilchuk C,Zeng W. Digital image watermarking using visual models[J]. Proc Spie,1997,3016: 100-111.
[61] HernándezJ, Amado M, Pérez-González F. DCT-domain watermarking techniques for still images: Detector performance analysis and a new structure[J]. IEEE Transaction on Image Processing, 2000,9(1): 55-68.
[62] JPEG2000: Multimedia and Hypemedia Standards Activity [EB/OL]. [2019-02-18]. http://www2.echo.lu/oii/en/oiiaug96.html#JPEG2000.
[63] Kundur D, Hatzinakos D. Digital watermarking using multi-resolution wavelet decomposition[J]. IEEE International Conference on Acoustic, Speech and Signal Processing, 1998,5: 2969-2972.
[64] Kundur D. Multiresolution digital watermarking: algorithms and implications for multimedia signals [D]. Toronto: University of Toronto, 1999.
[65] Xia X G, Boncelet C G, Arce G R. Wavelet transform based watermark for digital images[J]. Optics Express,1998,3(12): 497-511.
[66] Zhu Wenwu, Xiong Zixiang, Zhang Ya-Qin. Multiresolution watermarking for images andvideo[J]. IEEE Transaction on Circuits and Systems for Video Technology, 1999,9(4): 545-550.
[67] Swanson M D, Zhu B, Tewfik A H. Multiresolution scene-based video watermarking using perceptual models[J]. IEEE J. on selected areas in communications, 1998,16(4): 540-550.
[68] Barni M, Bartolini F, Piva A. Improved wavelet-based watermarking through pixel-wise masking [J]. IEEE Transaction Image Processing, 2001,10(5): 783-791.
[69] Pereira S, Pun T. Robust template matching for affine resist image watermarks[J]. IEEE Transaction on Image Processing, 2000,9(9): 1123-1129.
[70] Solachidis V, Pitas I. Circularly symmetric watermark embedding in 2-D DFT domain[J]. IEEE Transaction on Image Processing, 2001,10(11): 1741-1753.
[71] Deguillaume F, Csurka G, O'Ruanaidh J J K. Robust 3D DFT video watermarking[J]. Proceedings of Spie Security Watermarking,1999,(2): 365-376.
[72] Stankovic S, Duurovic I, Pitas I. Watermarking in the space/spatial—frequency domain using two-dimensional radon-wigner distribution[J]. IEEE Transaction on Image Processing, 2001,10(4): 650-658.
[73] Hernandez J J, Perez-Gonzalez F, Rodriguez J M. Performance analysis of a 2-Dmultipulse amplitude modulation scheme for data hiding and watermarking still images[J]. IEEE Journal on Selected Areas of Communications,1998,16(4): 510-524.
[74] Servetto S D, Podilchuk C I,Ramachandran K. Capacity issues in digital watermarking[J]. IEEE ICIP, 1998,1: 445-448.
[75] Moulin P. The role of information theory in watermarking and its application to image watermarking[J]. Signal Processing, 2001,81(6): 1121-1139.
[76] Su J K, Eggers J J, Girod B. Analysis of digital watermarks subjected to optimum linear filtering and additivenoise[J]. Signal Processing, 2001, 81(6): 1141-1175.
[77] Pérez-González F, Hernández J R, Balado F. Approaching the capacity limit in image watermarking: a perspective on coding techniques for data hiding applications[J]. Signal Processing, 2001, 81

(6): 1215-1238.
[78] Frank Hartung, Bernd Girod. Watermarking of Uncompressed and Compressed Video[J]. Signal Processing, 1998, 66(3): 283-301.
[79] Hartung F, Girod B. Digital watermarking of raw and compressedVideo[J]. Proceedings SPIE Digital Compression Technologies and Systems for Video Commun, 1996, 2952: 205-213.
[80] Hartung F, Girod B. Fast public-key watermarking of compressed Video[J]. IEEE International Conference on Image Processing, 1997, 1: 528-531.
[81] Hsu CT, Wu J L. Digital watermarking for video[J]. Signal Processing, 1997(5): 217-220.
[82] Langelaar G C, Langendijk R L, Biemond J. Real time labeling methods for MPEG compressed Video[J]. Proceeding of Symposiam Information Theory in the Benelux, 1997(5): 232-241.
[83] Swanson M, Zhu B, Tewfik A H. Multi-resolution Video watermarking using perceptual modelsand scenesugmentaticion [J]. IEEE International Conference on Image Processing, 1997, 2: 558-561.
[84] Langelaar G C, Langendijk R L, Biemond J. Real time labeling methods for MPEG compressed Video[J]. Proceeding of Symposiam Information Theory in the Benelux, 1997(5): 376-382.
[85] Swanson, Zhu B, Tewfik A H. Multi-resolution Video watermarking using perceptual modelsand scene sugmentaticion[J]. IEEE International Conference on Image Processing, 1997, 2: 558-561.
[86] Koch E, Zhao, Towards Robust J. Hidden Image CopyrightLabeling[J]. Piscataway: IEEE Press, 1995(6): 20-25.
[87] Linnartz J P. MPEG PTY marking. [J/OL]. [2019-02-20]. http://diva. eecs. berkeley. edu/linnartz/pty. html.
[88] Dittmann J, Stabenau M, Steinmetz R. Robust MPEG Video watermarking technologies[J/OL]. (1998-09-12) [2019-02-21]. https://www. researchgate. net/publication/221573619 _ Robust _ MPEG_Video_Watermarking_Technologies.
[89] Fridrich J. Methods for datahiding[J]. State Univ, 1997, 6: 210-221.
[90] Koch E, Zhao J. Toward robust and hidden image copyrightlabeling[J/OL]. (1997-06-12)[2019-02-22]. https://www. researchgate. net/publication/2314711 _ Towards _ Robust _ and _ Hidden _ Image_Copyright_Labeling.
[91] Wiegand T, Lightstone M, Mukherjee D. Rate distortion optimized mode selection for very low bit rate Video coding and the emerging H. 263 standard[J]. IEEE Transactions on Circuits and Systems for Video Technology, 1996, 6: 182-190.
[92] Langelaar G C. Watermarking Digital Image and VideoData[J]. IEEE Signal Processing Magazine, 2000, 9: 20-44.
[93] Justin Goshi, Alexander Mohr E, Eve Riskin A. Unequal Loss Protection for H. 263 Compressed Video[J]. In Processing of ICIP, 2003, 1: 367-370.
[94] Jordan F, Kutter M, Ebahimi T. Proposed of a watermarking technique for hiding/retrieving data in compressed and decompressed Video[J/OL]. [2019-02-24]. https://www. researchgate. net/publication/247285550_Proposal_of_a_watermarking_technique_for_hidingretrieving_data_in_compressed_and_decompressed_video.
[95] Cox I J, Kilian J, Leighton F T. Secure spread spectrum watermarking for multimedia[J]. IEEE Transactions on Image Processing, 1997, 6(12): 1674-1687.
[96] Darmstaedter V, Delaegle J F, Nicholson D. A block based watermarking technique for MPEG-2

signals: Optimization and validation on real digital TV distributionlinks[J/OL]. [2019-02-22]. https://link. springer. com/10. 1007%2F3-540-64594-2_95.

[97] Kalker T, Depovere G, Haitsma J. A Video watermarking system for broadcast monitoring[J/OL]. [2019-02-23]. http://www. zentralblatt-math. org/ioport/en/search/?q=an%3A10289349.

[98] Servetto, Podilchuk C I, Ramchandran K. Capacity issues in digital image watermarking[J]. Proceeding of the 1998 International Conference on Image Processing, 1998,1: 445-449.

[99] Lfgang,R B, Podilchuk. Perceptual watermarks for digital image and video[J]. Proceedings IEEE, 1999,87(7): 1108-1126.

[100] 王育民,梁传甲.信息与编码理论[M].西安:西北电讯工程学院出版社,1985.

[101] 杜江.信息隐藏的理论容量测度研究[J]. 信号处理,1999,15(10): 601-604.

[102] Watson A B. DCT Quantization Matrices Optimized for individual Images[J]. Piscataway: IEEE Press,1993,4: 202-216.

[103] Wolfgang R B, Delp E J. A watermark for digital images[J]. Proceedings IEEE International Conference on Image Processing, 1996,3: 219-222.

[104] Delaigie J F, De Vleeschouwer D, Macq B. Low cost perceptive digital picture watermarking method[J]. Proceedings of SPIE—The International Society for Optical, 1997(1): 153-167.

[105] Podilchuk C I, Zeng W. Perceptual watermarking of stillimages[J]. Multimedia Signal Processing,1997,6: 363-368.

[106] Voyatzis G, Pitas I. The use of watermarks in the protection of digital multimedia products[J]. Proceedings IEEE,1999,87(7): 1197-1207.

[107] Kuhn M G, Petitcolas F A P. StirMark. [2019-02-23]. http://www. cl. cam. ac. uk/～fapp2/watermarking/stirmark/.

[108] Deepa Kunder. Multi-resolution Digital Watermarking: Algorithms and Implications for Multimedia Signals[D]. Toronto: University of Toronto,2005.

[109] Ping Wah Wong. A Public Key Watermark for Image Verification and Authentication[J]. International Conference on Image Processing,1998,1: 455～458.

[110] Jiri Fridrich. Robust. Digital Watermarking Based on Key-Dependent Based Functions. Second International Workshop[J]. Oregon: Proceedings, 1998(5): 148-153.

[111] Jack Lacy, Schuyler. Intellectual Property Protection Systems and Digital Watermarking[J]. Oregon: Second International Workshop, 1998(6): 159-167.

[112] Alexand Herrigel Holger Petersen. Secure Copyright Protection Techniques for Digital Images[J]. Oregon: Second International Workshop, 1998(8): 170-187.

[113] 斯廷森 D R. 密码学——理论和实践[M]. 张文政,译. 成都:国防科学技术保密通信重点实验室,1997: 195-205.

[114] 王彩芬. 电子商务协议的形式分析与设计[D]. 西安:西安电子科技大学,2003.

[115] Andre Adelsbanch. Proving Ownership of Digital Content. Information Hiding[J]. Dresden: Third International Workshop,1999(2): 118-128.

[116] Scott Craver. Zero Knowledge Watermarking Detection. Information Hiding[J]. Dresden: Third International Workshop,1999(2): 101-115.

[117] Kinoshita Hirotsugu. An Image Digital Signature System with ZKIP for The Graph Isomorphish [J]. Proceedings International Conference on Image Proceeding,1996,9: 247-250.

[118] Bruce Schneier. Applied Cryptography protocols, algorithms and source code[M]. 吴世忠,译. 北

京：机械工业出版社，2003.

[119] Bruyndonckx O，Quisquater J J，Macq B. Spatial method for copyright labeling of digital images [J]. Proceedings International conference on Multimedia Computing and Systems，1996，6：514-521.

[120] ChenB，Wornell G. A cheievable performacnce of digital watermarking systems[J]. Proceedings IEEE International Conference in Multimedia Computer System，1999，1：13-18.

[121] Tirkel A Z，Osborne CF，Schyndel. Image watermarking—a spread spectrum application[J]. Proceedings IEEE International Symposium on Spread Spectrum Techniques and Applications，1997，2：13-16.

[122] Cox I J，Linnartz M G. Public watermarks and resistance to trampering[J]. Proceedings IEEE International Conference on Image Processing，1997，3：13-16.

[123] Piva A，BartoliniM，Cappellini V. DCT-based watermark recovering without resorting to the uncorrupted original image[J]. Proceedings IEEE International Conference on Image Processing，1997，1：520-523.

[124] Zhu W，Xiong Z，Zhang Y Q. multi-resolution watermarking for images and video：A unifiedapproach[J]. IEEE Transactions on Circuits and Systems for Video Technology，1998，1：153-156.

[125] Flikkema P G. Spread-spectrum techniques for wireless communications[J]. IEEE Signal Processing Magazine，1997，14：26-36.

[126] Chen B，Wornell G W. Dither mosulation：A new approach to digital watermarking and information embedding[A]. Proceedings SPIE Security and Watermarking of Multimedia Contents，1999：3657-3657.

[127] Cox I J，Kilian J，Leighton F T. Secure spread spectrum watermarking for multimedia[J]. IEEE Transactions on Image Processing，1997，6(12)：1674-1687.

[128] Hsu C T，Wu J L. Digital watermarking for video[J]. Proceedings International Conference on Digital Signal Processing，1997，6：217-220.

[129] Hsu C T，Wu J L. Hidden signatures in images[J]. Proceedings International Conference on Image Processing，1997，6：223-226.

[130] TaoB，Dickinson B. Adaptive watermarking in the DCT domain[J]. Proceedings International Conference on Acoustics，Speech and Signal Processing，1997，4：2985-2988.

[131] Caronni G. Assuring ownership rights for digital images[J/OL]. [2019-02-24]. https://link.springer.com/content/pdf/10.1007/978-3-322-91094-3_16.pdf.

[132] Bors A G，Pitas I. Image watermarking using DCT domain constraints[J]. Proceedings IEEE International Conference Image Processing，1996，3：231-234.

[133] Braudaway G W. Protecting publicly—available images with an invisiblewatermark[J]. IEEE International Conference Image Processing，1997(20)：524-531.

[134] ChenB，Wornell G W. An information theoretic approach to the design of robust digital watermarking systems[J]. Proceedings ICASSP'99，1999，4：322-335.

[135] Burgett S，Koch E，Zhao J. Copyright labeling of digitized image data[J]. IEEE Communication，2000(10)：94-100.

[136] Piva A，Barni M，Battolini F. DCT-based watermark recovering without resorting to the uncorrupted original image[J]. IEEE International Conference Image Processing，1997，10：520-527.

[137] Xia X G，Boncelet C G，Arce G R. A multi-resolution watermark for digital images[J]. IEEE

International Conference Image Processing,1997,1: 548-551.

[138] Xia X G, Boncelet C G, Arce G R. Wavelet transform based watermark for digital images[J]. Optics Express, 1998,3: 479-508.

[139] Kundur D, Hatzinakos D. A robust digital image watermarking method using wavelet based fusion [J]. IEEE International Conference on Image Processing, 1997,10: 544-547.

[140] Xia X G, Boncelet CG, Arce G R. A multi-resolution watermark for digital images[J]. IEEE International Conference Image Processing, 1997,10: 548-551.

[141] Pereira S, Pun T, Shelby P. Copyright techniques for digital images based on asymmetric cryptographic techniques[J]. Workshop on information Hiding,1998,4: 124-156.

[142] Herrigel A, Petersen H, Perteira S. Secure copyright protection techniques for digital images[J]. InformationHiding, 1998,1525: 169-190.

[143] Pereira S, Deguillanume F, Pun T. Template based recovery of Fourier-based watermarking using log-polar and log-logmaps[J]. Proceedings IEEE Multimedia Systems,1999,6: 7-11.

[144] Ruanaidh J J, Pun T. Rotation, scale and translation invariant spread spectrum digital image watermarking[J]. Signal Processing, 1998,66(3):303-119.

[145] Podilchuk C I,Zeng W. Image adaptive watermarking using visual models[J]. IEEE Journal on Selected Areas in Communications, 1999,16: 525-539.

[146] Wenjun Zeng. A Statistical Watermark Detection Technique Without Using Original Image for Resolving Rightful Ownerships of Digital Images[J]. IEEE Transaction on Image Processing, 1999, 8(11): 1534-1547.

[147] Podilchuk C I, Zeng W. Digital image watermarking using visual models[J]. Proceedings IS&T/SPIE Electronic Imaging: Human Vision and Electronic Imaging,1997,3016: 100-111.

[148] Peterson H A, Ahumada A J , Watson A B. Improved detection model for DCT coefficient quantization[J]. Proceedings SPIE Conference Human Vision, Visual Processing, and Digital Display IV, 1993, 1913:191-201.

[149] Tirkel A, van Schynel G R, Ho W. Electronicwatermark[J]. Proceedings DICTA,1993, 12: 666-672.

[150] Chiou-Ting Hus, Ja-Ling Wu. Hidden Digital Watermarks in Images[J]. IEEE Transactions on Image Processing, 1999,8(1): 58-68.

[151] Zhao J, Koch E. Embedding robust labels into images for copyright protection[J]. Proceedings International Congress Intellectual Property Rights for Specialized Information, Knowledge and New Technologies, 1995, 8: 242-251.

[152] Smith J R, Comiskey B O. Modulation and information hiding in images[J]. Lecture Notes in Computer Science: Information Hiding, 1996,1174: 207-226.

[153] Percival I, Vivaldi F. Arithmetical properties of strongly chaotic sustems[J]. Phusica 25D,1987: 105-130.

[154] Voyatzis G,Pitas I. Chaotic mixing of digital images and applications to watermarking[J]. Proceedings of ECMAST'96, 1996,2: 687-694.

[155] 杜江.信息隐藏与数字水印技术研究[D].西安:西安电子科技大学,2001.

[156] Teddy Furon and Pierre Duhamel. An Asymmetric Public Detection Watermarking Technique[J]. Information Hiding, Third International Workshop IH'99, 1999 : 89-98.

[157] Po-C, Ho-J Mike Wang, C.-C.JAY KUO. An Integrated Approach to image Watermarking and

JPEG-2000 Compression[J]. Journal of VLSI Signal Processing,2001,27: 35-53.
[158] Piva A, Bartolibi M, Cappellini V. DCT-based Watermark Recovering without Resorting to the Uncorrupted Original Image[J]. Proceedings of International Conference on Image Processing, 1997,1: 520-524.
[159] 陈丹,王继林,王育民. 一种利用原始图像嵌入的水印算法[J]. 全国信息隐藏学术研讨会论文(CIHW2002)集,2002,6: 180-183.
[160] Juan R, Hernandez, Fernando. Statistical Analysis of Watermarking Schemes for Copyright Protection of Images[J]. Proceedings of IEEE,1999,87(7): 1142-1166.
[161] 吴兆熊. 数字信号处理[M]. 西安: 西安交大出版社,2002.
[162] 范九伦. 模糊熵理论[M]. 西安: 西北大学出版社,1999.
[163] Nikolaidis N, Tsekeridou S, NikolaidisA. Applications of chaotic signal processing techniques to multimedia watermarking[J/OL]. [2019-02-25]. http://Poseidon. csd. auth. gr.
[164] Teddy Furon, Pierre Duhamel. An Asymmetric Public Detection Watermarking Technique[J]. Information Hiding, 1999,1: 89-98.
[165] Po-Chyisu, Houng-Jyh Mike Wang, Jay Kuo C C. An Integrated Approach to image Watermarking and JPEG-2000 Compression[J]. Journal of VLSI Signal Processing, 2001,27: 35-52.
[166] 张贤达,保铮. 通信信号处理[M]. 北京: 国防工业出版社,2000.
[167] Gary J, Sullivan, Thomas Wiegand. Rate-distortion optimization for video compression[J]. IEEE signal Processing Magazine,1998,98:81-82.
[168] Hashemzadeh M. Hiding information in videos using motion clues of featurepoints[J]. Computers & Electrical Engineering, 2018, 68: 14-25.
[169] Podilchuk C I, Zeng W. Image-adaptive watermarking using visual models[J]. IEEE Journal on selected areas in communication, 1998, 16(4): 525-539.
[170] Smith J R, Comiskey B O. Modulation and information hiding in images[J]. Lecture Notes in Computer Science: Information Hiding, 1996,1174: 207-226.
[171] Patrizio Campisi, arco Carli M. Blind Quality Assessment System for Multimedia Communications Using TracingWatermarking[J]. IEEE Transactions On Signal Processing, 2013,51(4): 996-1002.
[172] 哈尔滨工业大学. 哈尔滨工业大学信息检索研究中心(HIT CIR)语言技术平台共享资源和程序步骤[EB/OL]. [2009-6-9]http:// ir. hit. edu. cn / demo/ltp/Sharing_Plan. htm.
[173] 梅家驹, 竺一鸣, 高蕴琦,等. 同义词词林[M]. 上海: 上海辞书出版社, 1983.
[174] Jun Da. 现代汉语词频统计表[EB/OL]. [2019-02-25]. http://lingua. mtsu. edu/chinese-com Puting/statics.
[175] 甘灿,孙星明,刘玉玲,等. 一种改进的基于同义词替换的中文文本信息隐藏方法[N]. 东南大学学报(自然科学版),2007, 37(IS): 137-140.
[176] 卢开澄. 计算机密码学[M]. 北京: 清华大学出版社. 1998: 66-74.
[177] Arto Salomaa. 公钥密码学[M]. 北京: 国防工业出版社, 1995.
[178] Telenor Satellite Services. Adding Intra mode suitable for coding of flat regions[J]. JVT proposal, 2002,2:1-2.
[179] Real Networks. Two new directions for incaprediction[J]. JVT proposal,2000,5: 210-212.
[180] Telenor Satellite Services. New InCa prediction forchroma[J]. JVT proposal,2000,8: 266-278.
[181] Tekalp A M. Digital videoprocessing[M]. Chicago: Prentice Hall Press, 2015.

[182] Ramalingam M, Isa N A M. A data-hiding technique using scene-change detection for video steganography[J]. Computers & Electrical Engineering, 2016, 54: 423-434.
[183] 王丽娜，徐一波，翟黎明，等. 基于图像块复杂度的自适应视频运动矢量隐写算法[J]. 计算机学报,2017, 40(5): 1144-1156.
[184] 黄琳凯. Android 移动平台中的信息隐藏系统设计[J]. 网络安全技术与应用,2017,04: 129-131.
[185] 洪双喜. Android 平台隐私保护方法研究[D]. 北京：北京邮电大学，2017.
[186] Ya Kun Wei,Ling Xuan Zuo,Chun Bo Shao,et al. The Design of Instant Messaging System Based on Qt-Android System[J]. Advanced Materials Research,2014,2817(834): 13-15.
[187] 黄伟敏. Android 平台的即时通信系统客户端设计方案[J]. 现代电子技术，2011，34(16): 140-142.

图书资源支持

感谢您一直以来对清华版图书的支持和爱护。为了配合本书的使用，本书提供配套的资源，有需求的读者请扫描下方的“书圈”微信公众号二维码，在图书专区下载，也可以拨打电话或发送电子邮件咨询。

如果您在使用本书的过程中遇到了什么问题，或者有相关图书出版计划，也请您发邮件告诉我们，以便我们更好地为您服务。

我们的联系方式：

地　　址：北京市海淀区双清路学研大厦 A 座 701

邮　　编：100084

电　　话：010-83470236　010-83470237

资源下载：http://www.tup.com.cn

客服邮箱：2301891038@qq.com

QQ：2301891038（请写明您的单位和姓名）

资源下载、样书申请



书圈



扫一扫，获取最新目录



课　程　直　播

用微信扫一扫右边的二维码，即可关注清华大学出版社公众号“书圈”。